ARNAQUEOUFIABLE PRÉSENTE

Arnaque : le plan d’urgence

Réagir vite, limiter les dégâts
et reprendre le contrôle après une fraude

Guide exclusif ArnaqueOuFiable

ARNAQUEOUFIABLE PRÉSENTE

Arnaque : le plan d’urgence

Le guide pratique ArnaqueOuFiable pour réagir vite, limiter les dégâts et reprendre le contrôle après une fraude

Un guide exclusif proposé par ArnaqueOuFiable

Édition PDF premium - format A4

À PROPOS DE CE GUIDE

Un outil d’action immédiate

Vous venez de payer sur un faux site, de donner un mot de passe, de cliquer sur un lien douteux ou de parler à un faux conseiller ? Dans ces moments-là, le plus difficile n’est pas seulement l’arnaque. C’est la panique, la confusion, la honte, et la peur de faire encore pire.

Arnaque : le plan d’urgence a été conçu par ArnaqueOuFiable comme un guide d’action immédiate : procédures, checklists, messages prêts à copier, tableaux de priorités et arbres de décision. L’objectif est simple : vous aider à agir dans le bon ordre, sans paniquer, avec une méthode claire.

NAVIGATION

Sommaire

Introduction

Se faire arnaquer, ou penser qu'on vient de l'être, provoque souvent les mêmes réactions : sidération, stress, honte, colère, confusion. Certaines personnes se reprochent immédiatement d'avoir cliqué, répondu, payé ou fait confiance. D'autres restent bloquées, de peur d'aggraver la situation.

Ces réactions sont normales.

Le problème, c'est que les escrocs profitent précisément de cet état. Ils misent sur l'urgence, la pression, la peur, la culpabilité ou la précipitation. Et après l'arnaque initiale, ils tentent souvent d'aller plus loin : nouveau paiement, nouveau lien, nouveau faux conseiller, faux service d'aide, fausse récupération de fonds.

Dans ce moment-là, vous n'avez pas besoin d'un long cours théorique. Vous avez besoin d'un **plan clair**.

C'est exactement l'objectif de cet ebook proposé par **ArnaqueOuFiable**.

Depuis son site, **ArnaqueOuFiable** aide déjà les internautes à repérer les fraudes, comprendre les signaux d'alerte et identifier les pièges les plus courants. Ce guide va plus loin : il a été conçu comme une **boîte à outils d'urgence**, pour savoir quoi faire **immédiatement**, dans le bon ordre, selon votre situation.

Ici, vous ne trouverez pas de remplissage. Vous trouverez :

- des actions prioritaires ;
- des procédures concrètes ;
- des modèles de messages ;
- des checklists ;
- des arbres de décision ;
- des repères simples pour limiter les dégâts.

Le but n'est pas de promettre une solution miracle. Le but est de vous aider à **reprendre le contrôle**, étape par étape.

Ne cherchez pas à tout lire d'un coup. Allez d'abord à la partie qui correspond à votre situation. Faites le plus urgent. Conservez les preuves. Sécurisez l'essentiel. Revenez ensuite sur les étapes complémentaires.

Même si vous avez déjà commis une erreur, tout n'est pas perdu. Dans beaucoup de cas, une réaction rapide, ordonnée et factuelle permet de réduire fortement les conséquences.

Chapitre 1 - Que faire immédiatement

Le but de ce chapitre est simple : **vous aider à faire les bons gestes dans le bon ordre**.

Quand une arnaque vient d'avoir lieu, le risque principal n'est pas seulement ce que vous avez déjà perdu. Le vrai danger, c'est souvent **ce qui peut encore arriver dans les minutes et les heures qui suivent** : un second paiement, un accès à vos comptes, une utilisation de vos données, ou une nouvelle arnaque présentée comme une solution.

La règle à retenir

Si vous pensez avoir été arnaqué, appliquez d'abord cette logique :

1. **Stopper le contact**
2. **Limiter les dégâts**
3. **Conserver les preuves**
4. **Sécuriser l'argent**
5. **Sécuriser les comptes**
6. **Organiser la suite**

Ne cherchez pas à tout comprendre immédiatement. Commencez par **empêcher l'aggravation**.

Les 10 premières minutes

1. Coupez la conversation ou l'action en cours

Si l'arnaque est encore en train de se dérouler :

- quittez le site ;
- raccrochez ;
- arrêtez le chat ;
- fermez la fenêtre de paiement ;
- ne répondez plus.

Vous n'avez pas besoin d'être poli. Vous avez besoin de **reprendre la main**.

2. Ne payez plus rien

Même si on vous dit :

- “c’est la dernière étape” ;
- “il faut valider maintenant” ;
- “sinon votre argent sera perdu” ;
- “il faut payer pour débloquer le remboursement”.

N’envoyez plus rien.

3. Ne supprimez rien

Ne supprimez pas tout de suite :

- emails ;
- SMS ;
- captures ;
- reçus ;
- historique de discussion ;
- URL ;
- profils ;
- numéros.

Ces éléments peuvent devenir essentiels.

4. Identifiez en 60 secondes ce que vous avez donné

Posez-vous seulement ces questions :

- Ai-je donné de l’argent ?
- Ai-je donné un mot de passe ?
- Ai-je donné un code SMS ?
- Ai-je donné les données de ma carte ?
- Ai-je installé un logiciel ?
- Ai-je envoyé un document personnel ?
- Ai-je laissé quelqu’un accéder à mon appareil ?

Vous n’avez pas besoin d’être parfaitement sûr. Vous devez seulement repérer **la zone de risque principale**.

> **À faire tout de suite**
>
> - Couper le contact

- Ne plus cliquer
- Ne plus payer
- Noter ce que vous avez donné
- Commencer à sauvegarder les preuves

Ne faites surtout pas ceci

- Négocier avec l’escroc
- Chercher à “finir la procédure”
- Rappeler le faux numéro
- Cliquer sur un nouveau lien
- Supprimer les preuves par honte ou colère

Faire le tri très vite : niveau d’urgence

Urgence très élevée

Réagissez sans attendre si vous avez :

- donné votre carte bancaire ;
- validé un paiement ;
- donné un code SMS ;
- donné un mot de passe bancaire ou email ;
- installé un outil d’accès à distance ;
- parlé à un faux conseiller bancaire ou faux support ;
- envoyé une pièce d’identité dans un contexte douteux.

Urgence élevée

Réagissez dans la foulée si vous avez :

- rempli un formulaire après avoir cliqué ;
- donné des identifiants d’un compte important ;
- téléchargé un fichier douteux ;
- communiqué votre numéro et plusieurs informations personnelles.

Urgence modérée

Réagissez quand même, mais sans panique, si vous avez seulement :

- ouvert un email douteux sans cliquer ;

- visité un site suspect sans rien saisir ;
- donné une adresse email seule.

Les preuves à conserver immédiatement

Captures à faire tout de suite

Prenez des captures :

- du site ou de la page de paiement ;
- de l'email ou du SMS ;
- du numéro de téléphone ;
- du reçu ou de la confirmation de paiement ;
- du message de pression ou de menace ;
- de la conversation complète si possible.

Informations à noter

- date ;
- heure approximative ;
- montant ;
- moyen de paiement ;
- URL ;
- nom utilisé par l'escroc ;
- ce que vous avez communiqué.

Dossier simple à créer

Créez un dossier nommé par exemple :

Incident arnaque - [date]

Rangez-y :

- captures ;
- messages ;
- emails ;
- références de paiement ;
- notes.

> **À conserver comme preuve**
>
> - URL exacte

- Montant payé
- Libellé bancaire
- Numéro appelant
- Adresse email expéditrice
- Captures
- Historique de chat

Dans l’heure

Une fois le contact coupé et les premières preuves sauvegardées, passez à la phase essentielle : **limiter les dégâts concrets**.

1. Sécuriser l’argent

Si vous avez donné votre carte bancaire

- bloquez la carte si possible depuis l’application ;
- ou faites opposition ;
- ou contactez la banque ;
- vérifiez les opérations récentes.

Si vous avez validé un paiement douteux

- vérifiez le montant exact ;
- regardez s’il y a d’autres opérations ;
- notez le nom du bénéficiaire affiché.

Si vous avez fait un virement

- contactez la banque immédiatement ;
- signalez le caractère frauduleux ;
- demandez si une action reste possible ;
- notez la référence du dossier.

Si vous avez utilisé une plateforme de paiement

- ouvrez un signalement ;
- notez la référence ;
- gardez les captures.

2. Sécuriser les comptes critiques

Commencez dans cet ordre :

1. email principal ;
2. banque / paiement ;
3. compte opérateur ;
4. réseaux sociaux ;
5. marketplaces / comptes clients ;
6. autres comptes avec mot de passe réutilisé.

Pour chaque compte sensible :

- changez le mot de passe ;
- choisissez un mot de passe nouveau et unique ;
- vérifiez l'email de récupération ;
- vérifiez le numéro de récupération ;
- fermez les sessions ouvertes si possible ;
- activez la double authentification si vous le pouvez.

3. Sécuriser l'appareil si un accès ou un téléchargement est suspect

Si l'arnaque impliquait :

- un faux support technique ;
- un appel où vous avez suivi des instructions ;
- un logiciel installé ;
- une prise en main à distance ;

alors considérez votre appareil comme **potentiellement compromis**.

Réflexes utiles :

- coupez l'accès à distance si la session est encore active ;
- désinstallez l'outil seulement si vous l'identifiez clairement ;
- évitez les opérations sensibles sur cet appareil tant que le doute subsiste ;
- notez le nom du logiciel si vous le connaissez.

4. Prévenir les dommages en chaîne

Prévenez rapidement si nécessaire :

- un proche si votre messagerie ou votre réseau social a pu être compromis ;
- un conjoint si un moyen de paiement est partagé ;
- un employeur si une adresse pro est concernée.

Message type :

> Mon compte ou certaines de mes informations ont peut-être été compromis(es). Si vous recevez un message étrange de ma part, ne cliquez sur rien et ne payez rien. Je vous recontacte dès que possible.

5. Ouvrir un journal d'incident express

Notez :

- ce qui s'est passé ;
- ce que vous avez donné ;
- ce que vous avez payé ;
- ce que vous avez déjà fait ;
- les interlocuteurs contactés ;
- les références obtenues.

Dans les 24 heures

1. Faire les signalements utiles

Signalez la situation, selon le cas, à :

- la banque ;
- la plateforme de paiement ;
- le service client du site concerné ;
- la plateforme où le faux compte apparaît ;
- l'opérateur si un compte téléphonique est concerné ;
- un service officiel de signalement ;
- votre assurance si une protection adaptée existe.

2. Organiser votre dossier

Conservez ensemble :

- captures ;
- emails ;
- SMS ;
- reçus ;
- références ;
- chronologie ;
- réponses reçues.

3. Vérifier si l’arnaque continue

Surveillez :

- nouveaux appels ;
- messages de relance ;
- faux remboursements ;
- liens de “sécurisation” ;
- demandes de documents ;
- petits paiements tests.

4. Réduire le risque de seconde erreur

Posez-vous ces questions avant toute nouvelle action :

- Est-ce que cette personne représente vraiment l’organisme annoncé ?
- Est-ce que je vérifie par un autre canal ?
- Est-ce qu’on me demande encore de payer ?
- Est-ce qu’on me pousse à agir vite ?

5. Informer une personne de confiance

Ne gérez pas tout seul si vous êtes stressé. Une personne de confiance peut :

- relire un message ;
- vous aider à appeler ;
- prendre des notes ;
- vous empêcher de répondre dans la panique.

Dans les 7 jours

1. Contrôler l’aspect financier

- vérifiez vos relevés ;
- cherchez les petits débits suspects ;
- surveillez les paiements différés ;
- contrôlez les abonnements.

2. Contrôler les comptes et accès

- alertes de connexion ;
- nouveaux appareils ;
- changements de coordonnées ;
- demandes de réinitialisation ;

- messages envoyés à votre insu.

3. Finaliser la sécurisation minimale

- mots de passe critiques changés ;
- double authentification activée sur les comptes sensibles ;
- email principal renforcé ;
- appareils mis à jour.

4. Préparer la suite si le problème persiste

Faites un résumé propre :

- ce qui s'est passé ;
- ce que vous avez perdu ou partagé ;
- ce que vous avez déjà fait ;
- les dates ;
- les preuves disponibles ;
- les réponses reçues.

5. Rester attentif à la double peine

Méfiez-vous particulièrement :

- des faux récupérateurs de fonds ;
- des faux avocats ;
- des faux hackers ;
- des faux agents administratifs ;
- des faux assistants techniques.

Tableau de priorité rapide

Situation	Ce qu'il faut faire d'abord	Délai
J'ai payé par carte	Sécuriser la carte et vérifier les opérations	Immédiat
J'ai fait un virement	Contacter la banque	Immédiat
J'ai donné un mot de passe	Changer l'accès concerné	Immédiat
J'ai donné un code SMS	Vérifier le compte lié	Immédiat
J'ai installé un outil	Couper l'accès et éviter les usages sensibles	Immédiat
J'ai envoyé un document	Conserver le contexte et surveiller	Très rapide

Situation	Ce qu'il faut faire d'abord	Délai
J'ai seulement ouvert un email	Ne rien cliquer et rester vigilant	Rapide

Chapitre 2 - Identifier le type d’arnaque

Quand on vient d’être piégé, on ne sait pas toujours exactement **ce qui s’est passé**. Ce chapitre sert à faire un **tri rapide**.

L’idée n’est pas de poser un diagnostic parfait. L’idée est de répondre à cette question :

Dans quelle catégorie mon problème ressemble-t-il le plus ?

Pour chaque cas, retenez :

- les **symptômes typiques** ;
- le **niveau d’urgence** ;
- le **risque principal** ;
- la **première action prioritaire**.

1. Faux site marchand

Symptômes typiques

- prix très attractifs ;
- site rassurant en apparence, mais peu vérifiable ;
- service client flou ;
- confirmation douteuse ;
- colis absent ou faux suivi.

Niveau d’urgence

Élevé à très élevé si vous avez payé par carte.

Risque principal

- perte d’argent ;
- carte compromise ;
- abonnement caché ;
- collecte de données.

Première action

Vérifier immédiatement le paiement et sécuriser le moyen de paiement utilisé.

2. Phishing bancaire

Symptômes typiques

- email, SMS ou appel prétendant venir de votre banque ;
- urgence de sécurité ;
- lien vers une page de connexion ;
- demande d'identifiants ou de code SMS.

Niveau d'urgence

Très élevé

Risque principal

- accès à votre compte bancaire ;
- validation d'opérations ;
- fraude en cascade.

Première action

Contacter votre banque sans attendre et sécuriser l'accès au compte.

3. Faux support technique

Symptômes typiques

- appel ou fenêtre d'alerte prétendant que votre appareil est infecté ;
- demande d'installer un outil ;
- demande d'ouvrir votre banque ou vos réglages ;
- paiement demandé pour "réparer".

Niveau d'urgence

Très élevé

Risque principal

- prise de contrôle de l'appareil ;
- vol d'identifiants ;
- observation de données sensibles.

Première action

Couper l'accès à distance et considérer l'appareil comme potentiellement compromis.

4. Faux investissement / crypto / trading

Symptômes typiques

- promesse de gains rapides ;
- conseiller très insistant ;
- faux tableau de bord ;
- impossibilité de retirer ;
- nouvelles sommes demandées pour “débloquer”.

Niveau d’urgence

Très élevé

Risque principal

- pertes répétées ;
- nouvelles demandes de paiement ;
- collecte de documents ;
- faux récupérateurs ensuite.

Première action

Cesser tout versement immédiatement.

5. Arnaque sentimentale

Symptômes typiques

- relation rapide en ligne ;
- demande d’aide financière ;
- histoires urgentes et émotionnelles ;
- pression affective.

Niveau d’urgence

Élevé à très élevé selon ce qui a déjà été envoyé.

Risque principal

- pertes répétées ;
- emprise émotionnelle ;
- exploitation de documents ou comptes.

Première action

Stopper l'envoi d'argent et figer les échanges.

6. Arnaque au colis / faux SMS de livraison

Symptômes typiques

- message parlant d'un colis bloqué ;
- petits frais à payer ;
- lien de paiement ;
- imitation d'un transporteur connu.

Niveau d'urgence

Modéré à élevé, mais **très élevé** si vous avez payé ou saisi vos données.

Risque principal

- vol de carte bancaire ;
- collecte de données ;
- abonnement ou débit frauduleux.

Première action

Si vous avez payé ou saisi des données, sécuriser immédiatement le moyen de paiement et les comptes liés.

7. Faux conseiller / faux service client

Symptômes typiques

- numéro trouvé en urgence ;
- rappel d'un prétendu service officiel ;
- demande de codes ou de paiements ;
- forte pression.

Niveau d'urgence

Très élevé

Risque principal

- manipulation sous stress ;
- vol d'accès ;
- validation de paiements ;

- installation d’outils.

Première action

Rompre le contact et sécuriser immédiatement ce que vous avez montré, donné ou validé.

8. Faux abonnement / essai piégé

Symptômes typiques

- essai prétendument gratuit ;
- petit paiement suivi d’un plus gros ;
- résiliation difficile ;
- conditions floues.

Niveau d’urgence

Élevé

Risque principal

- débits répétés ;
- conservation de la carte ;
- frais cachés.

Première action

Identifier si un abonnement a été activé et empêcher les prochains débits.

9. Vol de carte ou données bancaires

Symptômes typiques

- données de carte communiquées ;
- débit inconnu ;
- petit paiement test ;
- plusieurs opérations inhabituelles.

Niveau d’urgence

Très élevé

Risque principal

- multiplication rapide des débits ;
- abonnements frauduleux ;

- usage répété de la carte.

Première action

Bloquer ou faire opposition sur la carte concernée.

10. Compte en ligne compromis

Symptômes typiques

- mot de passe refusé ;
- email de modification inconnu ;
- activité inhabituelle ;
- proches contactés à votre place.

Niveau d’urgence

Élevé à très élevé

Risque principal

- perte de compte ;
- usurpation ;
- récupération d’autres comptes.

Première action

Tenter de reprendre l’accès et sécuriser d’abord l’email principal si lié.

11. Arnaque à l’identité

Symptômes typiques

- envoi de pièce d’identité ;
- justificatif de domicile ;
- selfie ou vidéo ;
- demande présentée comme une “simple vérification”.

Niveau d’urgence

Élevé

Risque principal

- usurpation d’identité ;
- ouverture de comptes ;
- fraude ciblée ultérieure.

Première action

Conserver toutes les preuves du contexte d’envoi et noter exactement ce qui a été transmis.

Tableau de tri rapide

Situation repérée	Niveau d’urgence	Risque principal	Première priorité
Faux site marchand	Élevé à très élevé	Paiement / carte compromise	Vérifier et sécuriser le paiement
Phishing bancaire	Très élevé	Accès au compte / validations	Contacter la banque
Faux support technique	Très élevé	Appareil compromis	Couper l’accès à distance
Faux investissement	Très élevé	Versements répétés	Stopper tout paiement
Arnaque sentimentale	Élevé à très élevé	Pertes + emprise	Couper les envois
Faux colis	Modéré à élevé	Données bancaires ou personnelles	Sécuriser si données saisies
Faux conseiller	Très élevé	Manipulation + vol d’accès	Couper et sécuriser
Faux abonnement	Élevé	Débits récurrents	Empêcher les prochains débits
Vol de carte	Très élevé	Multiplication des débits	Bloquer / opposer la carte
Compte compromis	Élevé à très élevé	Perte d’accès / usurpation	Reprendre l’accès
Documents envoyés	Élevé	Usurpation d’identité	Tracer et surveiller

Chapitre 3 - Plan d’action par situation

Ce chapitre transforme les grands principes en **protocoles concrets**. La logique ArnaqueOuFiable reste toujours la même :

Stopper -> sécuriser -> conserver -> signaler -> surveiller

1. J’ai payé sur un faux site

Étape 1 - Vérifier le paiement

- montant ;
- bénéficiaire affiché ;
- opérations en attente ;
- autres débits éventuels.

Étape 2 - Sécuriser le moyen de paiement

- blocage ou opposition si la carte a été exposée ;
- signalement à la plateforme de paiement si concerné.

Étape 3 - Conserver les preuves

- URL ;
- page produit ;
- page de paiement ;
- email de confirmation ;
- captures ;
- échanges.

Étape 4 - Contacter les bons acteurs

1. banque ou émetteur de carte ;
2. plateforme de paiement ;
3. site marchand si cela aide à constituer le dossier ;
4. service de signalement si utile.

Étape 5 - Vérifier ensuite

- petits débits tests ;
- paiements répétés ;
- abonnement caché ;

• relances du faux site.

À faire tout de suite

- Vérifier si la carte est exposée
- Bloquer ou opposer si nécessaire
- Garder les preuves
- Ne pas repayer pour “débloquer”

2. J’ai payé par carte dans un contexte douteux

Étape 1

Bloquer temporairement la carte ou faire opposition.

Étape 2

Vérifier :

- opérations du jour ;
- opérations en attente ;
- petits montants anormaux ;
- paiements récurrents.

Étape 3

Contacter la banque avec une demande claire :

- sécuriser la carte ;
- vérifier les opérations ;
- indiquer la procédure à suivre.

Étape 4

Noter la référence du contact.

Étape 5

Surveiller les jours suivants.

Script court :

> Bonjour, je pense avoir exposé les données de ma carte dans un contexte frauduleux. Je souhaite sécuriser immédiatement la carte et vérifier les opérations récentes. Pouvez-vous m'indiquer la marche à suivre et enregistrer ce signalement ?

3. J'ai fait un virement à un escroc

Étape 1

Contacter la banque immédiatement.

Étape 2

Demander :

- si le virement est déjà exécuté ;
- si une action reste possible ;
- quelle procédure interne appliquer.

Étape 3

Rassembler :

- preuve du virement ;
- échanges ;
- faux contrat ;
- IBAN du bénéficiaire ;
- captures.

Étape 4

Stopper toute suite de paiement.

Étape 5

Vérifier si vos identifiants ou documents ont aussi été exposés.

4. J'ai donné mes identifiants

Étape 1

Changer le mot de passe du compte concerné.

Étape 2

Sécuriser l'email principal si lié.

Étape 3

Vérifier :

- email de récupération ;
- numéro de récupération ;
- appareils connectés ;
- sessions ouvertes.

Étape 4

Déconnecter les sessions si possible.

Étape 5

Changer aussi les autres comptes où le mot de passe était réutilisé.

> **Vérification rapide**
> Le mot de passe servait-il aussi pour mon email ? Ma banque ? D'autres comptes ? Si oui, changez tout ce qui est lié.

5. J'ai donné un code SMS ou un code de validation

Étape 1

Identifier le compte ou l'action concernée.

Étape 2

Vérifier immédiatement :

- opération réalisée ;
- connexion ;
- modification de sécurité ;
- appareil connecté.

Étape 3

Contacter l'organisme réel si le compte est sensible.

Étape 4

Modifier les accès sans attendre.

Étape 5

Surveiller les heures suivantes.

6. J’ai parlé à un faux conseiller bancaire ou faux service client

Étape 1

Couper immédiatement le contact.

Étape 2

Lister ce que vous avez montré ou validé :

- mot de passe ;
- code SMS ;
- opération ;
- outil installé ;
- écran bancaire affiché.

Étape 3

Contacter l’organisme réel par un canal officiel.

Étape 4

Sécuriser selon l’exposition :

- carte ;
- compte ;
- email ;
- appareil.

Étape 5

Noter le scénario précis.

7. J’ai installé un logiciel ou donné un accès à distance

Étape 1

Couper l’accès si la session est encore active.

Étape 2

Ne plus faire d’opérations sensibles depuis l’appareil.

Étape 3

Repérer ce qui a été installé :

- nom du logiciel ;
- heure ;
- action demandée.

Étape 4

Désinstaller uniquement si vous identifiez clairement l'outil.

Étape 5

Sécuriser les comptes ouverts pendant la session.

8. J'ai cliqué sur un lien frauduleux

Cas A - J'ai cliqué mais je n'ai rien saisi

- fermer la page ;
- ne rien télécharger ;
- conserver une capture si utile ;
- surveiller les relances.

Cas B - J'ai saisi des informations

- identifier ce que vous avez saisi ;
- traiter selon la donnée la plus sensible ;
- conserver l'URL exacte.

Cas C - J'ai téléchargé un fichier

- ne plus l'ouvrir ;
- noter le nom du fichier ;
- éviter les usages sensibles sur l'appareil si doute ;
- surveiller le comportement de l'appareil.

9. J'ai envoyé une pièce d'identité ou des documents personnels

Étape 1

Lister précisément ce qui a été envoyé.

Étape 2

Conserver le contexte exact :

- annonce ;
- faux site ;
- email ;
- nom utilisé ;
- date.

Étape 3

Vérifier s'il y a aussi un risque financier ou d'accès.

Étape 4

Préparer un résumé écrit.

Étape 5

Surveiller la suite :

- nouvelles demandes ;
- nouvelles pièces demandées ;
- contacts liés au même dossier.

10. J'ai donné seulement mon email ou mon numéro

Étape 1

Ne rien donner de plus.

Étape 2

Surveiller les messages entrants.

Étape 3

Être attentif aux tentatives de réinitialisation si l'email est sensible.

Étape 4

Conserver le premier contact.

11. J’ai accepté un faux abonnement ou un essai piégé

Étape 1

Vérifier les débits.

Étape 2

Identifier le commerçant exact.

Étape 3

Empêcher la répétition :

- résiliation si le canal est fiable ;
- blocage du moyen de paiement si nécessaire ;
- signalement.

Étape 4

Surveiller les jours suivants.

12. Je suis dans une arnaque à l’investissement ou à la crypto

Étape 1

Stopper tout versement.

Étape 2

Refuser tout “déblocage” payant.

Étape 3

Rassembler le dossier :

- captures du tableau de bord ;
- messages ;
- noms ;
- promesses de gains ;
- preuves de versement ;
- documents transmis.

Étape 4

Sécuriser aussi les accès ou documents donnés.

Étape 5

Bloquer le canal de manipulation.

> **Signal d'alerte majeur**
> Si on vous demande encore de payer pour récupérer ce qui vous appartient déjà, considérez cela comme une prolongation de l'arnaque.

13. Je pense qu'un proche est victime

Étape 1

Commencer sans accusation.

Étape 2

Poser 3 questions simples :

- Qu'est-ce que tu as donné ?
- Qu'est-ce que tu as payé ?
- Est-ce qu'un compte ou un appareil a été exposé ?

Étape 3

Traiter d'abord le plus grave.

Étape 4

Aider à conserver les preuves.

Étape 5

Répartir les tâches :

- une personne appelle ;
- une personne note ;
- une personne rassemble les captures.

Chapitre 4 - Modèles prêts à copier-coller

Ce chapitre vous fait gagner du temps quand vous êtes stressé. Les modèles sont courts, réalistes et adaptables.

1. Email à la banque après paiement frauduleux

Objet : Signalement d'opération frauduleuse / demande de sécurisation urgente

> Bonjour,
>
> Je vous contacte pour signaler une opération que je considère comme frauduleuse ou réalisée dans un contexte d'arnaque.
>
> Date : [date]
> Montant : [montant]
> Moyen de paiement : [carte / virement / autre]
> Contexte : [faux site / faux conseiller / lien frauduleux / autre]
>
> Je vous demande de sécuriser immédiatement la situation et de m'indiquer la marche à suivre pour la suite du dossier.
>
> Merci de me confirmer la prise en compte de ce signalement.
>
> Cordialement,
> [Nom]
> [Coordonnées]

2. Demande de blocage de carte

> Bonjour,
> Je pense avoir exposé les données de ma carte dans un contexte frauduleux. Je demande le blocage immédiat de la carte concernée et la vérification des opérations récentes.
>
> Merci de me confirmer la prise en compte de ma demande.
>
> [Nom]
> [4 derniers chiffres si utile]

3. Contestation d’opération

Objet : Contestation d’opération non autorisée ou frauduleuse

Bonjour,

Je conteste l’opération suivante, que je considère comme non autorisée ou liée à une fraude :
Date : [date]
Montant : [montant]
Libellé : [libellé exact]

Cette opération est liée à [description courte].

Merci de m’indiquer la procédure applicable et les éléments à fournir.

Cordialement,
[Nom]

4. Signalement après exposition d’identifiants

Bonjour,

Je pense avoir communiqué mes identifiants ou informations de sécurité dans un contexte frauduleux.
Je souhaite sécuriser immédiatement mon accès et vérifier qu’aucune opération ou modification anormale n’a été effectuée.

Merci de m’indiquer les actions urgentes à effectuer.

Cordialement,
[Nom]

5. Relance si la première réponse est floue

Bonjour,

Je reviens vers vous concernant mon signalement du [date] relatif à une fraude ou à une opération contestée.

Ma demande porte sur :

- la sécurisation du moyen de paiement ou du compte ;
- la vérification des opérations ;
- la procédure à suivre.

Merci de me confirmer précisément les prochaines étapes et la référence du dossier.

Cordialement,
[Nom]

6. Message au service client après achat sur un site douteux

Bonjour,

Je vous contacte au sujet de la commande suivante : [numéro], effectuée le [date] pour un montant de [montant].

Je n'ai à ce jour reçu [aucune confirmation fiable / aucun suivi crédible / aucune réponse claire], ce qui m'amène à contester la fiabilité de cette transaction.

Merci de me confirmer immédiatement :

- l'état réel de la commande ;
- les coordonnées complètes du vendeur ;
- les modalités de résolution.

Cordialement,
[Nom]

7. Demande d'arrêt d'un abonnement douteux

Bonjour,

Je demande l'arrêt immédiat de tout abonnement, prélèvement récurrent ou reconduction lié à mon inscription du [date].

Merci de me confirmer par écrit la résiliation effective et l'absence de nouveau débit.

Cordialement,
[Nom]

8. Signalement d’un compte ou vendeur frauduleux

Bonjour,

Je souhaite signaler un compte ou une annonce que je considère comme frauduleux(se).

Nom du compte / annonce : [nom]
Lien : [lien]
Motif : [faux vendeur / usurpation / demande de paiement frauduleuse / autre]

Merci de vérifier rapidement ce contenu et de prendre les mesures nécessaires.

Cordialement,
[Nom]

9. Demande de suppression d’un faux compte utilisant votre identité

Bonjour,

Un compte semble utiliser mon identité, mon nom, mes photos ou mes informations sans autorisation.

Lien du compte : [lien]
Éléments concernés : [nom / photo / contenu / autre]

Je demande la suppression rapide de ce compte ou de ce contenu frauduleux.

Merci de me confirmer la prise en compte du signalement.

Cordialement,
[Nom]

10. Résumé court d’incident

Le [date] à [heure approximative], j’ai été en contact avec [site / numéro / profil / email] dans le cadre de [achat / appel / message / investissement / autre].

J’ai communiqué : [carte / mot de passe / code / document / autre].
J’ai payé : [oui/non, montant si oui].

Après vérification, je considère qu’il s’agit d’une arnaque ou d’une tentative de fraude.

Je conserve les preuves utiles : captures, messages, URL, références de paiement.

11. Message à un proche si votre compte a pu être compromis

Bonjour,

Je préfère vous prévenir : un de mes comptes ou certaines de mes informations ont peut-être été compromis(es).

Si vous recevez un message étrange, une demande d’argent, un lien ou un document inhabituel de ma part, ne répondez pas et ne cliquez sur rien.

Je vous confirmerai directement toute information importante.

12. Script téléphonique pour appeler sa banque

Bonjour. Je vous appelle parce que je pense avoir été victime d’une fraude.

J’ai [payé sur un faux site / communiqué mes données de carte / donné un code / donné mes identifiants / parlé à un faux conseiller].

Je souhaite sécuriser immédiatement la situation, vérifier les opérations récentes et connaître la procédure à suivre.

Pouvez-vous m’indiquer les actions urgentes et me donner une référence de dossier ?

À noter pendant l’appel

- heure ;
- nom du service ;
- numéro du dossier ;
- action faite ;
- prochaine étape annoncée.

Chapitre 5 - Checklists pratiques

Ces checklists sont pensées comme des **outils d'exécution**. Ne cherchez pas à tout cocher d'un coup. Commencez par :

1. ce qui protège l'argent ;
2. ce qui protège les accès ;
3. ce qui protège les preuves.

Checklist 1 - J'ai payé sur un faux site

Immédiatement

- ☐ Arrêter tout contact avec le site
- ☐ Ne plus payer une seconde fois
- ☐ Faire des captures du site, du produit, du paiement et des emails
- ☐ Noter l'URL exacte
- ☐ Noter le montant, la date et l'heure

Dans l'heure

- ☐ Vérifier le paiement sur l'application bancaire
- ☐ Vérifier s'il y a d'autres opérations
- ☐ Bloquer ou sécuriser la carte si nécessaire
- ☐ Conserver l'email de confirmation ou le reçu

Dans les 24 heures

- ☐ Contacter la banque ou la plateforme de paiement
- ☐ Garder une trace écrite des démarches
- ☐ Vérifier s'il existe un abonnement ou un débit récurrent
- ☐ Préparer un dossier simple

Pendant 7 jours

- ☐ Surveiller les petits débits tests
- ☐ Surveiller les nouveaux paiements inconnus
- ☐ Se méfier des relances du faux site
- ☐ Surveiller un éventuel abonnement caché

Checklist 2 - J’ai donné mes identifiants

Immédiatement

- ☐ Identifier le compte concerné
- ☐ Changer le mot de passe
- ☐ Utiliser un mot de passe nouveau et unique
- ☐ Ne plus utiliser le lien reçu

Dans l’heure

- ☐ Vérifier les sessions ouvertes
- ☐ Déconnecter les appareils inconnus si possible
- ☐ Vérifier l’email et le numéro de récupération
- ☐ Activer la double authentification si possible

Dans les 24 heures

- ☐ Contrôler les autres comptes liés
- ☐ Vérifier si le mot de passe était réutilisé
- ☐ Prévenir les proches si le compte peut envoyer des messages à votre place
- ☐ Conserver les messages de phishing

Pendant 7 jours

- ☐ Surveiller les tentatives de connexion

- ☐ Surveiller les emails de sécurité
- ☐ Vérifier qu’aucune donnée n’a été modifiée
- ☐ Vérifier qu’aucun message n’est parti à votre insu

Checklist 3 - J’ai cliqué sur un lien frauduleux

Si je n’ai rien saisi

- ☐ Fermer la page
- ☐ Ne rien télécharger
- ☐ Conserver une capture si utile
- ☐ Surveiller les relances

Si j’ai saisi des informations

- ☐ Identifier ce que j’ai saisi
- ☐ Si carte : sécuriser le moyen de paiement
- ☐ Si mot de passe : changer l’accès
- ☐ Si code : vérifier le compte concerné
- ☐ Si document : conserver la preuve de l’envoi
- ☐ Noter l’URL exacte

Si j’ai téléchargé un fichier

- ☐ Ne plus l’ouvrir
- ☐ Noter son nom
- ☐ Éviter les usages sensibles sur l’appareil si doute
- ☐ Surveiller le comportement de l’appareil

Checklist 4 - On me met la pression pour payer vite

- ☐ On me dit que c’est urgent
- ☐ On me dit que je n’ai que quelques minutes

- ☐ On me menace de blocage ou de perte
- ☐ On me demande de ne parler à personne
- ☐ On me demande de payer avant toute vérification

Réflexes

- ☐ Stopper la conversation
- ☐ Ne rien payer dans l'urgence
- ☐ Vérifier par un autre canal
- ☐ Demander un second avis
- ☐ Relire calmement le message

Checklist 5 - Je pense qu'un proche est victime

Signaux faibles

- ☐ Le proche paraît honteux ou nerveux
- ☐ Il veut agir seul et vite
- ☐ Il a envoyé de l'argent à quelqu'un d'inconnu
- ☐ Il parle d'un investissement miraculeux
- ☐ Il a reçu un appel "officiel" très pressant

À faire

- ☐ Parler calmement
- ☐ Ne pas accuser
- ☐ Poser trois questions : qu'as-tu donné ? qu'as-tu payé ? un compte ou un appareil a-t-il été exposé ?
- ☐ Conserver les preuves
- ☐ Répartir les tâches

Checklist 6 - J’ai parlé à un faux conseiller

- ☐ Raccrocher
- ☐ Ne pas rappeler
- ☐ Noter le numéro utilisé
- ☐ Noter ce qui a été demandé
- ☐ Noter ce que j’ai validé ou montré
- ☐ Contacter l’organisme réel
- ☐ Vérifier les opérations récentes
- ☐ Changer les accès si besoin
- ☐ Sécuriser la carte si nécessaire

Checklist 7 - J’ai installé un outil ou donné un accès à distance

- ☐ Couper la session si elle est encore active
- ☐ Arrêter toute opération sensible sur l’appareil
- ☐ Noter le nom du logiciel
- ☐ Conserver les messages ou captures
- ☐ Vérifier si la banque, l’email ou un compte sensible a été ouvert pendant la session
- ☐ Changer les accès aux comptes ouverts
- ☐ Surveiller les connexions inhabituelles

Checklist 8 - J’ai envoyé une pièce d’identité ou des documents

- ☐ Lister exactement les documents envoyés
- ☐ Noter à qui et par quel canal
- ☐ Conserver le message ou le site qui a demandé ces documents
- ☐ Faire des captures
- ☐ Vérifier s’il y a eu aussi une demande d’argent ou d’accès

- ☐ Préparer un résumé clair
- ☐ Surveiller les relances ou demandes complémentaires

Checklist 9 - Version ultra courte “urgence absolue”

Les 5 gestes prioritaires

- ☐ Stopper le contact
- ☐ Ne plus payer
- ☐ Conserver les preuves
- ☐ Sécuriser argent ou comptes
- ☐ Noter ce qui s’est passé

Les 5 questions à se poser

- ☐ Ai-je payé ?
- ☐ Ai-je donné un mot de passe ?
- ☐ Ai-je donné un code ?
- ☐ Ai-je installé quelque chose ?
- ☐ Ai-je envoyé un document ?

Les 5 erreurs à éviter

- ☐ Payer une seconde fois
- ☐ Supprimer les preuves
- ☐ Rappeler le faux numéro
- ☐ Cliquer sur un nouveau lien
- ☐ Croire à un faux service de récupération

Chapitre 6 - Erreurs fréquentes à éviter

Après une arnaque, beaucoup de dégâts supplémentaires viennent des **mauvaises réactions dans les heures qui suivent**.

1. Paniquer et agir dans le désordre

Pourquoi c'est dangereux

Vous perdez :

- du temps ;
- des preuves ;
- de la clarté ;
- parfois votre seule fenêtre d'action utile.

Bon réflexe

Revenir à l'ordre simple :

1. couper le contact ;
2. sécuriser l'argent ;
3. sécuriser les comptes ;
4. conserver les preuves ;
5. organiser la suite.

2. Supprimer trop vite les preuves

Pourquoi c'est dangereux

Ensuite, il devient plus difficile de :

- prouver la chronologie ;
- retrouver l'URL ;
- montrer le contexte ;
- appuyer un signalement.

Bon réflexe

Capturer avant d'effacer.

3. Rappeler un faux numéro ou continuer la discussion

Pourquoi c’est dangereux

Vous :

- confirmez que vous êtes joignable ;
- vous exposez à une nouvelle manipulation ;
- prolongez l’emprise.

Bon réflexe

Couper le contact. Ne pas négocier.

4. Payer une seconde fois

Pourquoi c’est dangereux

Le deuxième paiement n’est presque jamais le dernier.

Bon réflexe

Dès qu’on vous demande de payer pour corriger, débloquer ou récupérer, considérez cela comme **une prolongation de l’arnaque**.

5. Croire à un faux service de récupération

Pourquoi c’est dangereux

Les faux récupérateurs ciblent précisément les victimes déjà fragilisées.

Signes très mauvais

- paiement d’avance ;
- garantie de récupération ;
- forte pression ;
- identité floue ;
- demande de nouveaux documents.

Bon réflexe

Ne payez rien pour une prétendue récupération.

6. Cliquer sur un nouveau lien reçu après l’arnaque

Pourquoi c’est dangereux

C’est souvent la **deuxième phase** :

- vol d’identifiants ;
- nouveau paiement ;
- téléchargement ;
- collecte de documents.

Bon réflexe

Ne cliquez sur aucun nouveau lien lié au dossier sans vérification indépendante.

7. Publier trop d’informations personnelles

Pourquoi c’est dangereux

Vous exposez encore plus de données exploitables.

Bon réflexe

Masquer les données sensibles avant tout partage.

8. Réutiliser un mot de passe “temporairement”

Pourquoi c’est dangereux

Le risque ne s’arrête pas au premier compte compromis.

Bon réflexe

Utiliser immédiatement un mot de passe **nouveau et unique**.

9. Penser qu’un petit montant n’est pas grave

Pourquoi c’est dangereux

Un petit débit peut être :

- un test ;
- un abonnement ;
- le début d’une série.

Bon réflexe

Traiter un petit débit suspect comme un vrai signal d’alerte.

10. Attendre plusieurs jours avant d’agir

Pourquoi c’est dangereux

Le temps profite souvent :

- aux paiements qui s’enchaînent ;
- aux accès frauduleux ;
- aux changements de compte.

Bon réflexe

Même si vous n’êtes pas sûr à 100 %, sécurisez l’essentiel immédiatement.

11. Vouloir tout résoudre seul

Pourquoi c’est dangereux

Une victime seule :

- oublie des étapes ;
- se fatigue plus vite ;
- reste plus vulnérable à la pression.

Bon réflexe

Prévenir au moins une personne de confiance.

12. Chercher à tout comprendre avant d’agir

Pourquoi c’est dangereux

Cela retarde les gestes urgents.

Bon réflexe

D’abord sécuriser, ensuite analyser.

Tableau récapitulatif

Erreur	Pourquoi c’est dangereux	Bon réflexe
Paniquer et agir dans le désordre	Perte de temps et d’efficacité	Revenir aux priorités
Supprimer les preuves	Dossier affaibli	Capturer avant d’effacer
Rappeler l’escroc	Nouvelle manipulation	Couper le contact
Payer une seconde fois	Escalade de la fraude	Refuser tout nouveau paiement
Croire un récupérateur	Double arnaque	Vérifier hors canal
Cliquer sur un nouveau lien	Deuxième phase de fraude	Ne rien ouvrir sans vérification
Publier trop d’infos	Nouvelle exposition	Masquer les données
Réutiliser un mot de passe	Cascade de compromissions	Utiliser un mot de passe unique
Ignorer un petit débit	Signal précoce raté	Le traiter comme un vrai risque
Attendre trop longtemps	Dégâts amplifiés	Agir sur l’essentiel

Chapitre 7 - Comment éviter la double peine

La première fraude n'est pas toujours la fin. Dans de nombreux cas, **la première arnaque ouvre la porte à une seconde**, parfois encore plus dangereuse.

Le mécanisme est simple : quelqu'un sait ou prétend savoir que vous avez déjà été victime. Il utilise cette information pour vous approcher au moment où vous êtes le plus vulnérable.

1. Le faux récupérateur de fonds

Ce qu'il promet

- "Nous pouvons récupérer vos fonds"
- "Votre argent a été localisé"
- "Il faut agir vite avant qu'il disparaisse"

Ce qu'il demande

- frais de dossier ;
- avance ;
- documents supplémentaires ;
- accès à vos comptes ;
- nouveau paiement.

Réflexe

Refuser tout paiement de récupération.

2. Le faux avocat ou faux juriste

Son discours typique

- "Votre dossier peut être pris en charge"
- "Il faut payer pour lancer le recours"
- "Vos fonds sont bloqués dans une procédure"

Vérifications minimales

- identité vérifiable ;
- existence indépendante de la structure ;
- coordonnées cohérentes ;

- absence de pression immédiate.

Réflexe

Ne jamais s'engager uniquement parce que le discours semble professionnel.

3. Le faux hacker ou faux expert technique

Promesses typiques

- "Je peux tracer les fonds"
- "Je peux récupérer votre compte"
- "Je peux pirater les escrocs"

Réflexe

Refuser toute "solution technique miracle", surtout si elle implique secret, urgence et paiement d'avance.

4. Le faux agent administratif

Angle d'attaque

- "Votre dossier a été signalé"
- "Il manque une pièce"
- "Il faut régulariser"
- "Des frais sont nécessaires"

Réflexe

Toute démarche sérieuse doit pouvoir être **vérifiée indépendamment**.

5. Le faux service d'assistance

Après un faux support ou un compte compromis, une nouvelle personne peut prétendre "finir le travail".

Réflexe

Ne laissez jamais une deuxième personne "vous aider" à distance sans vérification indépendante.

6. Le faux enquêteur, faux journaliste ou faux modérateur

Objectif réel

Créer de la confiance pour :

- obtenir votre histoire complète ;
- récupérer vos preuves ;
- récupérer de nouvelles données ;
- préparer une nouvelle tentative.

Réflexe

Rester factuel et refuser tout basculement vers paiement, accès ou documents supplémentaires.

7. Les signaux qui doivent faire refuser immédiatement

- nouveau paiement demandé ;
- récupération garantie ;
- pression temporelle ;
- secret exigé ;
- impossibilité de vérifier hors du message ;
- nouvelles données sensibles réclamées.

> **Vérification rapide**
> Si une “solution” cumule **promesse + urgence + paiement + secret**, traitez-la comme **très probablement frauduleuse**.

8. Le protocole anti-double peine

1. Ne répondez pas dans l’urgence
2. Posez-vous 4 questions :
    - Qui est cette personne exactement ?
    - Comment vérifier son identité ?
    - Pourquoi demande-t-elle de payer ou d’agir vite ?
    - Que risque-t-on si on attend 15 minutes ?

3. Vérifiez hors du canal initial
4. Refusez tout paiement de récupération
5. Notez la tentative
6. Coupez le contact si le doute persiste

Tableau des faux secours les plus fréquents

Faux secours	Promesse	Ce qu'il demande	Réflexe
Faux récupérateur de fonds	Récupérer l'argent	Frais, avance	Refuser tout paiement
Faux avocat	Lancer une procédure	Paiement rapide, documents	Vérifier indépendamment
Faux hacker	Récupérer fonds ou compte	Paiement, accès	Couper immédiatement
Faux agent administratif	Régulariser	Pièces, frais	Vérifier hors message
Faux service d'assistance	Corriger le problème	Installation, accès	Refuser sans vérification
Faux modérateur / enquêteur	Aider	Informations sensibles	Rester prudent

Chapitre 8 - Arbres de décision

Ce chapitre est une **boussole d'urgence**. Prenez uniquement la situation qui correspond au geste le plus grave que vous avez fait.

1. Si j'ai payé par carte, alors...

J'ai payé par carte dans un contexte douteux

→ Le paiement est-il visible ?

- Oui → vérifier montant, libellé et autres opérations
- Non → vérifier s'il est en attente

→ Les données de la carte ont-elles été saisies sur un site douteux ?

- Oui → sécuriser la carte sans attendre
- Non → chercher une autre origine possible

→ Y a-t-il d'autres débits ?

- Oui → urgence forte
- Non → surveiller les jours suivants

→ Me réclame-t-on un nouveau paiement ?

- Oui → ne rien payer
- Non → garder les preuves et continuer les démarches

2. Si j'ai fait un virement, alors...

→ Le virement est-il très récent ?

- Oui → contacter la banque immédiatement
- Non → contacter quand même la banque

→ L'escroc réclame-t-il un second virement ?

- Oui → arrêt immédiat
- Non → surveiller toute nouvelle demande

→ Ai-je aussi donné des documents ou identifiants ?

- Oui → traiter aussi ces risques
- Non → concentrer d'abord l'action sur le virement

3. Si j’ai seulement donné mon email, alors…

→ Ai-je donné seulement l’email ?

- Oui → risque limité mais réel
- Non → passer à l’arbre correspondant à la donnée plus sensible

→ Ai-je reçu ensuite des relances ou liens ?

- Oui → ne rien cliquer, conserver la trace
- Non → rester vigilant

→ Cet email est-il mon email principal ?

- Oui → surveiller les tentatives de réinitialisation
- Non → vigilance simple

4. Si j’ai donné mon mot de passe, alors…

→ Quel compte est concerné ?

- Email principal → urgence très élevée
- Banque / paiement → urgence très élevée
- Réseau social / autre → urgence élevée

→ Le mot de passe était-il réutilisé ailleurs ?

- Oui → changer aussi les autres comptes
- Non → sécuriser d’abord le compte compromis

→ Ai-je encore accès au compte ?

- Oui → changer le mot de passe immédiatement
- Non → lancer la récupération

5. Si j’ai donné un code SMS, alors…

→ Le code concernait-il un compte sensible ?

- Oui → urgence très élevée
- Non → urgence élevée

→ Ai-je vu une opération ou une connexion après cela ?

- Oui → vérifier immédiatement le compte concerné
- Non → vérifier quand même les accès

→ M’a-t-on demandé un second code ?

- Oui → ne rien transmettre de plus
- Non → modifier les accès sans attendre

6. Si j’ai cliqué sur un lien frauduleux, alors…

Cas 1 - J’ai cliqué mais je n’ai rien fait d’autre

→ fermer la page
→ ne rien télécharger
→ conserver une capture si utile
→ surveiller les relances

Cas 2 - J’ai cliqué et j’ai saisi quelque chose

→ identifier ce qui a été saisi
→ traiter selon la donnée la plus sensible
→ conserver l’URL

Cas 3 - J’ai cliqué et j’ai téléchargé un fichier

→ ne plus l’ouvrir
→ noter le nom
→ éviter les usages sensibles sur l’appareil si doute

7. Si j’ai installé un logiciel ou donné un accès à distance, alors…

→ La session est-elle encore ouverte ?

- Oui → la couper immédiatement
- Non → considérer quand même l’appareil comme exposé

→ Ai-je ouvert ma banque, mon email ou un compte sensible ?

- Oui → sécuriser ces comptes en priorité
- Non → vérifier quand même les activités récentes

→ L’escroc me recontacte-t-il ?

- Oui → couper tout échange
- Non → rester vigilant

8. Si j’ai envoyé une pièce d’identité, alors…

→ Quel document ai-je envoyé ?

- pièce d’identité ;
- justificatif ;
- selfie / vidéo ;
- RIB / IBAN ;
- plusieurs éléments à la fois.

→ Ai-je aussi payé ou donné un accès ?

- Oui → traiter d’abord l’argent ou l’accès
- Non → documenter précisément ce qui a été envoyé

→ Me demande-t-on d’autres pièces ?

- Oui → arrêt immédiat
- Non → conserver toutes les traces et surveiller

9. Si mon compte en ligne semble compromis, alors…

→ Quel compte est concerné ?

- Email principal → priorité absolue
- Banque / paiement → priorité absolue
- Réseau social / messagerie → priorité élevée
- Marketplace / autre → priorité élevée

→ Le mot de passe est-il refusé ?

- Oui → tenter récupération et sécuriser les comptes liés
- Non → vérifier quand même les sessions et paramètres

→ Mes proches reçoivent-ils des messages à ma place ?

- Oui → les prévenir immédiatement
- Non → rester vigilant

10. Si un proche est impliqué, alors…

→ Le proche a-t-il payé ?

- Oui → traiter le volet financier en priorité
- Non → passer à la suite

→ Le proche a-t-il donné un mot de passe, un code ou un accès ?

- Oui → sécuriser les comptes
- Non → vérifier s'il s'agit surtout d'une tentative

→ Le proche est-il sous pression ou dans le déni ?

- Oui → rester calme et traiter l'urgence concrète
- Non → avancer ensemble sur les étapes

11. Arbre ultra court : que faire selon ce que j'ai donné ?

Ce que j'ai donné	Première priorité
Argent par carte	Sécuriser la carte et vérifier les opérations
Argent par virement	Contacter la banque immédiatement
Mot de passe	Changer l'accès tout de suite
Code SMS	Vérifier le compte lié immédiatement
Accès à distance	Couper la session et sécuriser les comptes ouverts
Pièce d'identité	Conserver les preuves et surveiller
Email seul	Ne rien donner de plus et surveiller

Chapitre 9 - Mini plan de prévention pour ne plus rechuter

Le but n'est pas de devenir expert. Le but est de mettre en place **quelques réflexes simples et durables**.

1. Ne pas payer dans la précipitation

Avant tout paiement inhabituel, posez-vous ces 3 questions :

- Qui me demande de payer exactement ?
- Puis-je vérifier autrement ?
- Pourquoi faut-il payer tout de suite ?

Règle simple : pas de paiement important ou inhabituel sans vérification hors du message reçu.

2. Ne jamais utiliser un lien reçu pour se connecter à un compte sensible

Pour l'email principal, la banque, l'opérateur ou une plateforme de paiement :

- passez par votre application habituelle ;
- ou tapez l'adresse vous-même ;
- ou utilisez un favori déjà enregistré.

3. Séparer les mots de passe importants

Les comptes qui doivent avoir un mot de passe différent :

- email principal ;
- banque ;
- plateforme de paiement ;
- compte opérateur ;
- comptes professionnels sensibles.

4. Se méfier des demandes “d’aide” après un problème

Après une arnaque ou un blocage :

- ne faites pas confiance au premier interlocuteur ;
- vérifiez indépendamment ;
- refusez les solutions miracles.

5. Prendre 2 minutes avant d’envoyer un document sensible

Avant d’envoyer :

- pièce d’identité ;
- justificatif ;
- selfie ;
- RIB ;
- document administratif ;

demandez-vous :

- à qui exactement je l’envoie ;
- pourquoi il est demandé ;
- puis-je vérifier le destinataire ;
- suis-je sous pression ?

6. La sécurisation minimale qui change vraiment les choses

Protéger l’email principal

- mot de passe unique ;
- email de récupération correct ;
- numéro de récupération correct ;
- double authentification si possible.

Activer la double authentification sur les comptes sensibles

Commencez par :

- email principal ;

- banque ;
- plateforme de paiement ;
- réseau social principal.

Mettre à jour les appareils

- téléphone ;
- ordinateur ;
- navigateur ;
- applications importantes.

Vérifier les alertes bancaires

Activez les notifications utiles si votre banque le permet.

Nettoyer les vieux comptes inutiles

Surtout ceux avec carte enregistrée ou accès oubliés.

7. Les vérifications systématiques à adopter

Avant de cliquer

- Est-ce que j'attendais ce message ?
- Puis-je passer autrement ?
- L'urgence est-elle crédible ?

Avant de payer

- Qui reçoit l'argent ?
- Le site ou l'interlocuteur est-il vérifié ?
- Suis-je poussé à agir vite ?

Avant d'appeler

- D'où vient ce numéro ?
- Est-ce un numéro trouvé dans l'urgence ?
- Puis-je le retrouver par un canal fiable ?

Avant d'envoyer un document

- Pourquoi est-il demandé ?
- Le destinataire est-il vérifié ?
- Suis-je sous pression ?

Vérification rapide
Urgence + paiement + pression = pause immédiate

8. Routine anti-arnaque en 5 minutes par mois

Une fois par mois

- vérifier les derniers paiements inhabituels ;
- relire les comptes sensibles ;
- contrôler les alertes de sécurité ;
- regarder si un vieux abonnement traîne ;
- vérifier que l'email principal est bien sécurisé.

Tous les quelques mois

- revoir les mots de passe vraiment critiques si besoin ;
- vérifier les coordonnées de récupération ;
- faire du tri dans les comptes inutiles.

9. Mini plan familial ou pour proches vulnérables

Règle familiale utile :

Aucun paiement urgent, aucun code, aucun document important sans vérification avec une personne de confiance.

10. Les 5 ajustements utiles après incident

- changer les accès les plus sensibles ;
- renforcer l'email principal ;
- mettre en place une vérification avant paiement ;
- garder un contact de confiance ;
- conserver cet ebook comme plan de crise.

Tableau du minimum vital anti-rechute

Habitude	Effort	Impact
Ne pas payer dans l'urgence	Faible	Très fort

Habitude	Effort	Impact
Passer par l’application ou le site tapé manuellement	Faible	Très fort
Séparer les mots de passe critiques	Moyen	Très fort
Activer la double authentification sur les comptes sensibles	Moyen	Fort
Vérifier les alertes bancaires	Faible	Fort
Faire une pause avant d’envoyer un document	Faible	Fort
Demander un second avis	Faible	Fort

Annexes pratiques

Annexe A - Fiche mémo ultra courte

Les 5 gestes immédiats

1. Couper le contact
2. Ne plus payer
3. Conserver les preuves
4. Sécuriser l'essentiel
5. Noter ce qui s'est passé

Les 5 erreurs à éviter

- payer une seconde fois ;
- supprimer les preuves ;
- rappeler le faux numéro ;
- cliquer sur un nouveau lien ;
- attendre plusieurs jours.

Les 5 questions à se poser

- Ai-je payé ?
- Ai-je donné un mot de passe ?
- Ai-je donné un code SMS ?
- Ai-je installé un outil ?
- Ai-je envoyé un document ?

Les 5 priorités

1. argent
2. accès
3. codes
4. appareil
5. documents

Annexe B - Tableau récapitulatif des priorités

Ce qui s'est passé	Niveau d'urgence	Priorité immédiate	Suite à vérifier
J'ai payé par carte	Très élevé	Sécuriser la carte	Débits tests, abonnements
J'ai fait un virement	Très élevé	Contacter la banque	Nouvelles demandes
J'ai donné un mot de passe	Très élevé	Changer l'accès	Comptes réutilisés
J'ai donné un code SMS	Très élevé	Vérifier le compte lié	Connexions, validations
J'ai installé un outil	Très élevé	Couper l'accès	Comptes ouverts pendant la session
J'ai envoyé une pièce d'identité	Élevé	Tracer l'envoi	Relances, usurpation
J'ai donné seulement mon email	Modéré	Ne rien donner de plus	Relances, réinitialisations

Annexe C - Que faire selon ce que j'ai donné / perdu / partagé

Carte bancaire

- vérifier les opérations ;
- sécuriser la carte ;
- conserver les preuves ;
- surveiller les jours suivants.

Virement

- contacter la banque ;
- conserver la preuve ;
- noter le bénéficiaire ;
- refuser tout nouveau paiement.

Mot de passe

- changer immédiatement le mot de passe ;
- sécuriser l'email lié ;

- vérifier les sessions ;
- changer les comptes réutilisés.

Code SMS

- identifier le compte concerné ;
- vérifier les opérations ou connexions ;
- changer les accès ;
- contacter l'organisme réel si sensible.

Email

- ne rien donner de plus ;
- surveiller les relances ;
- surveiller les tentatives de réinitialisation si l'email est principal.

Numéro de téléphone

- surveiller appels et SMS suspects ;
- se méfier des faux conseillers ;
- ne jamais valider un code sans contexte clair.

Pièce d'identité

- noter exactement ce qui a été envoyé ;
- conserver le contexte ;
- garder les messages ;
- surveiller les demandes complémentaires.

Justificatif de domicile

- conserver la preuve d'envoi ;
- noter le destinataire et le contexte ;
- surveiller les relances.

Selfie ou vidéo

- noter la date et le contexte ;
- conserver la plateforme ou le profil utilisé ;
- surveiller la suite.

RIB / IBAN

- conserver le contexte d'envoi ;
- vérifier si d'autres données ont été données ;
- surveiller les relances.

Accès à distance

- couper la session ;
- arrêter les usages sensibles ;
- sécuriser les comptes ouverts ;
- garder les preuves.

Argent envoyé dans une arnaque à l'investissement

- stopper tout versement ;
- garder le tableau de bord et les messages ;
- refuser tout déblocage payant ;
- couper le contact.

Annexe D - Glossaire ultra simple

Arnaque : manœuvre destinée à vous tromper pour obtenir de l'argent, des accès ou des informations.
Phishing : message ou site qui imite un service connu pour récupérer vos identifiants ou vos données.
Faux site marchand : site qui semble vendre normalement mais sert à voler de l'argent ou des données.
Opposition carte : action visant à bloquer une carte.
Contestation d'opération : démarche pour signaler un paiement frauduleux ou non autorisé.
Double authentification : protection supplémentaire demandant un second élément, souvent un code.
Code SMS : code temporaire qui peut valider une opération ou une connexion.
Accès à distance : outil permettant à quelqu'un de voir ou contrôler votre appareil.
Compte compromis : compte auquel une personne non autorisée a pu accéder.
Usurpation d'identité : utilisation frauduleuse de vos informations pour se faire passer pour vous.
Faux récupérateur de fonds : escroc qui promet de récupérer votre argent après une première fraude.
Abonnement piégé : offre qui déclenche des débits récurrents ou cachés.
Vérification indépendante : contrôle effectué hors du message reçu, via un canal fiable connu de vous.
Preuve utile : capture, email, SMS, URL, reçu, référence, date ou heure.

Annexe E - Journal d’incident prêt à remplir

Fiche d’incident

Date de l’incident :

.....

Heure approximative :

.....

Type d’arnaque supposé :

.....

Canal utilisé :

- ☐ Email
- ☐ SMS
- ☐ Téléphone
- ☐ Site web
- ☐ Réseau social
- ☐ Messagerie
- ☐ Autre : .....

Nom utilisé par l’interlocuteur / le site :

.....

Adresse du site / lien / profil / numéro :

.....

Ce que j’ai donné

- ☐ Carte bancaire
- ☐ Virement
- ☐ Mot de passe
- ☐ Code SMS
- ☐ Email
- ☐ Téléphone
- ☐ Pièce d’identité

- ☐ Justificatif de domicile
- ☐ RIB / IBAN
- ☐ Selfie / vidéo
- ☐ Accès à distance
- ☐ Autre : .....

Ce que j'ai payé

Montant :

.....

Moyen de paiement :

.....

Libellé visible / référence :

.....

Ce que j'ai déjà fait

- ☐ J'ai coupé le contact
- ☐ J'ai conservé les preuves
- ☐ J'ai sécurisé ma carte
- ☐ J'ai changé un mot de passe
- ☐ J'ai vérifié mes comptes
- ☐ J'ai contacté un organisme
- ☐ J'ai prévenu un proche
- ☐ Autre : .....

Interlocuteurs déjà contactés

Date	Organisme / service	Réponse obtenue	Référence

Éléments de preuve conservés

- ☐ Captures d'écran
- ☐ Emails

- ☐ SMS
- ☐ Reçus
- ☐ Référence de paiement
- ☐ URL
- ☐ Historique de chat
- ☐ Numéro appelant
- ☐ Fichier téléchargé
- ☐ Autre : .....

Prochaines actions à faire

1. .....
2. .....
3. .....
4. .....
5. .....

Annexe F - Page de notes d’urgence

Contacts utiles

Banque :

.....

Opérateur :

.....

Email principal / service concerné :

.....

Personne de confiance :

.....

Références de dossier

Organisme	Date	Référence

Comptes à vérifier

- ☐ Email principal
- ☐ Banque
- ☐ Plateforme de paiement
- ☐ Réseau social
- ☐ Marketplace
- ☐ Compte opérateur
- ☐ Autre : .....

Points à surveiller pendant 7 jours

- ☐ Nouveaux débits
- ☐ Tentatives de connexion
- ☐ Messages suspects
- ☐ Relances du faux interlocuteur
- ☐ Demandes de paiement complémentaires
- ☐ Changement de paramètres
- ☐ Activité inhabituelle sur mes comptes

Annexe G - Tableau “Que faire en priorité ?”

Si j’ai…	Je fais d’abord…	Puis…
payé par carte	je sécurise la carte	je surveille les opérations
fait un virement	je contacte la banque	je conserve toutes les preuves
donné un mot de passe	je change l’accès	je sécurise les comptes liés
donné un code SMS	je vérifie le compte concerné	je change les accès
installé un outil	je coupe l’accès / j’arrête l’usage sensible	je sécurise les comptes ouverts
envoyé une pièce d’identité	je conserve le contexte	je surveille les relances
	je ne donne rien de plus	

Si j’ai…	Je fais d’abord…	Puis…
donné seulement mon email		je surveille les tentatives suivantes

Annexe H - Fiche “minimum absolu si je suis débordé”

Les 3 actions minimales

1. Couper le contact
2. Conserver les preuves
3. Sécuriser la carte ou le compte le plus exposé

Les 3 choses à ne pas faire

1. Ne pas repayer
2. Ne pas cliquer sur un nouveau lien
3. Ne pas croire à un faux sauvetage

Les 3 choses à noter

1. ce que vous avez donné
2. ce que vous avez payé
3. à quelle heure environ

Conclusion

Une arnaque peut créer un sentiment de chaos. Le but de ce guide n'est pas de vous promettre l'impossible. Il est de vous donner un **ordre d'action clair** quand tout devient flou.

La méthode **ArnaqueOuFiable** tient en quelques principes :

- stopper ;
- sécuriser ;
- conserver ;
- vérifier ;
- surveiller.

Une réaction parfaite n'existe pas. Une réaction **méthodique** peut en revanche faire une vraie différence.

Gardez ce guide. Relisez les fiches mémo. Imprimez les checklists si nécessaire. Et surtout, souvenez-vous de cette idée simple :

Une action utile faite tout de suite vaut mieux qu'une panique totale.

Guide exclusif ArnaqueOuFiable

À conserver, relire et utiliser dès qu’un doute apparaît ou qu’une situation devient confuse.

ArnaqueOuFiable prolonge ici son expertise avec une approche plus opérationnelle : procédures, checklists, scripts et plans d’action pour aider les victimes à réagir vite et méthodiquement.

Ce document a été conçu comme un support à garder sous la main : pratique, rassurant, structuré et immédiatement utile.