

Arnaques au téléphone, par SMS et sur WhatsApp : comprendre les méthodes utilisées

Aujourd'hui, votre numéro de téléphone ne sert plus seulement à recevoir des appels. Il est aussi utilisé pour vérifier votre identité, récupérer vos comptes et recevoir des codes de sécurité. S'il est détourné, les conséquences peuvent aller bien au-delà de la perte du réseau et de sa fonction première qui est de téléphoner.

Christian Pelardy - Home Computer Maintenance
10 septembre 2026

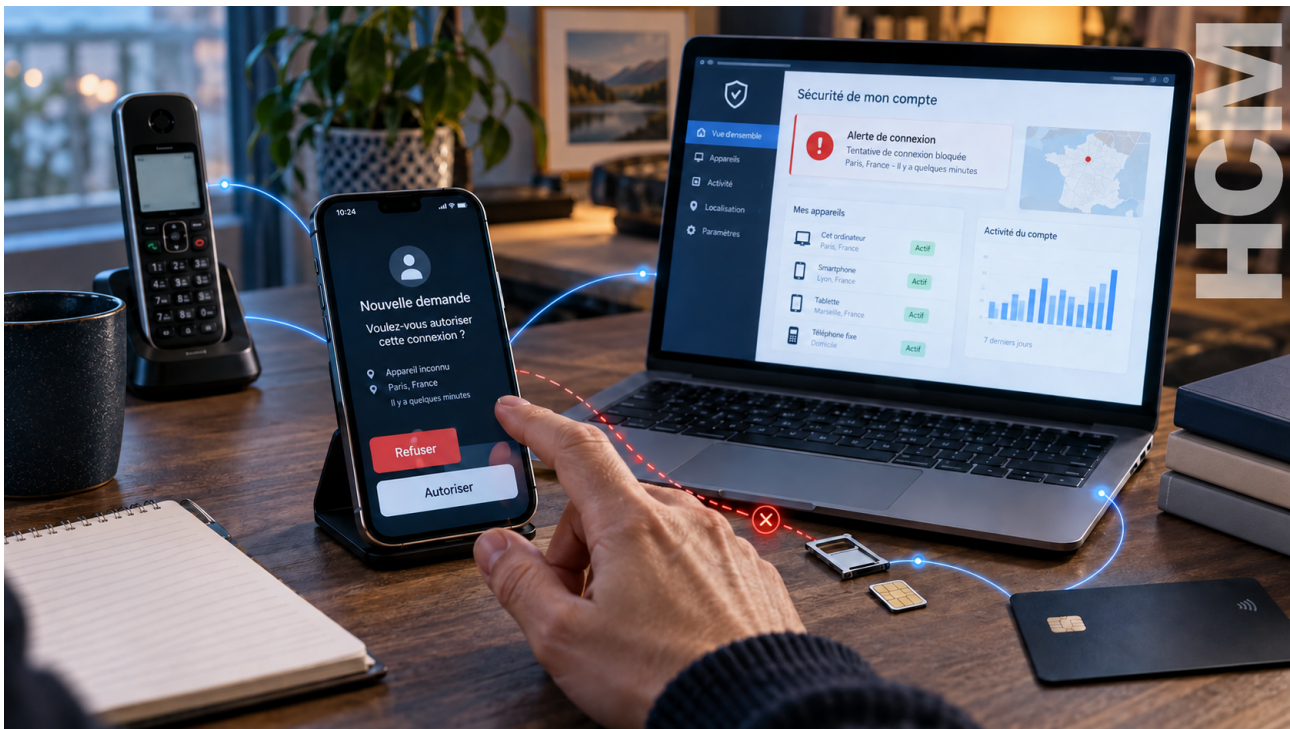
Un SMS qui semble envoyé par votre enfant. Un appel affichant le numéro de votre banque. Un prétendu technicien qui veut "réparer" votre téléphone. Un code WhatsApp que l'on vous demande de transmettre. Une ligne mobile qui cesse soudainement de fonctionner.

Ces situations ne correspondent pas toutes à la même arnaque. Certaines reposent uniquement sur le mensonge. D'autres permettent réellement de détourner un compte, une ligne téléphonique ou une validation bancaire. Plusieurs peuvent aussi être combinées : un SMS vole d'abord vos identifiants, puis un faux conseiller vous appelle, et un code reçu sur votre téléphone termine l'opération.

L'objectif de cet article n'est donc pas seulement de dresser une liste de pièges. Il est de montrer, pour chaque méthode :

- ce que fait réellement l'escroc ;
- ce qu'il doit déjà connaître ou posséder ;
- ce que votre action peut lui permettre de faire ;
- ce qu'il ne peut pas faire automatiquement ;
- comment vérifier sans prendre de risque ;
- et comment réagir selon ce qui s'est effectivement passé.

Règle essentielle : ne jugez jamais une demande uniquement d'après le nom, le logo, la voix ou le numéro affiché. Vérifiez par un autre canal que vous choisissiez vous-même.



Le mécanisme commun : vous faire accomplir l'action décisive

Dans de nombreuses arnaques téléphoniques, le fraudeur ne " pirate " pas immédiatement votre téléphone. Il commence par créer une situation crédible et urgente : un enfant en difficulté, une fraude bancaire en cours, un colis bloqué, un compte menacé, un appareil infecté.

Son objectif est de vous faire accomplir vous-même une action utile :

- répondre et confirmer que le numéro est actif ;
- cliquer sur un lien ;
- saisir un mot de passe ou des coordonnées bancaires ;
- communiquer un code à usage unique ;
- accepter une notification dans une application ;
- ajouter un bénéficiaire ou effectuer un virement ;
- scanner un QR code ;
- installer un outil de prise en main à distance ;
- rappeler un numéro surtaxé.

L'urgence sert à empêcher la vérification. Les informations personnelles connues par l'interlocuteur servent à créer la confiance. Mais connaître votre nom, votre banque, votre adresse ou les derniers chiffres de votre carte ne prouve pas que la personne travaille pour l'organisme concerné. Ces données peuvent avoir été volées lors d'une intrusion dans les serveurs ou le système informatique d'une entreprise, d'une administration ou d'un service que vous utilisez. Elles peuvent aussi provenir d'un ancien hameçonnage, d'un compte compromis ou de documents volés.

Ces fuites sont malheureusement courantes en ce moment en France. La CNIL a reçu 6 167 notifications de violations de données en 2025, un record, et la moitié des incidents déclarés relevaient d'un piratage. Une fuite ne contient pas forcément des mots de passe, mais lorsque c'est le cas, les fraudeurs essaient souvent le mot de passe volé sur d'autres sites. C'est pour cela que je recommande à tous mes clients de ne jamais utiliser le même mot de passe partout. Chaque compte doit avoir son propre mot de passe. Ainsi, si un service est piraté, les autres comptes ne tombent pas avec lui. ([CNIL, rapport annuel 2025](#) ; [Cybermalveillance.gouv.fr, bien gérer ses mots de passe](#))

1. Le SMS " Papa, Maman, j'ai perdu mon téléphone "

Le message prend généralement cette forme :

" Coucou maman, j'ai cassé mon téléphone. Voici mon numéro temporaire. Écris-moi sur WhatsApp, c'est urgent. "

Il est souvent envoyé en masse, sans que l'escroc sache réellement si le destinataire a un enfant. Si vous répondez comme à votre fils ou à votre fille, vous lui fournissez vous-même une première information. Il poursuit alors la conversation en évitant parfois les détails vérifiables, puis invente une urgence : téléphone à remplacer, facture à payer, compte momentanément bloqué, virement à effectuer ou codes de coupons PCS, Transcash ou Neosurf à transmettre.

Ce qui s'est réellement passé

Dans le scénario le plus courant, le téléphone de votre enfant n'a pas été piraté. Le fraudeur utilise simplement un autre numéro et usurpe son identité par écrit.

On peut supposer que ce nouveau numéro provient d'une carte prépayée, d'une ligne obtenue sous une fausse identité, d'un numéro détourné ou d'un service permettant d'émettre des messages. Ce sont des possibilités crédibles, mais le SMS seul ne permet pas de savoir laquelle est vraie. Autrement dit, on peut expliquer ces différentes possibilités, mais on ne peut pas affirmer d'où vient le numéro simplement en lisant le message.

La vérification qui coupe court à l'arnaque

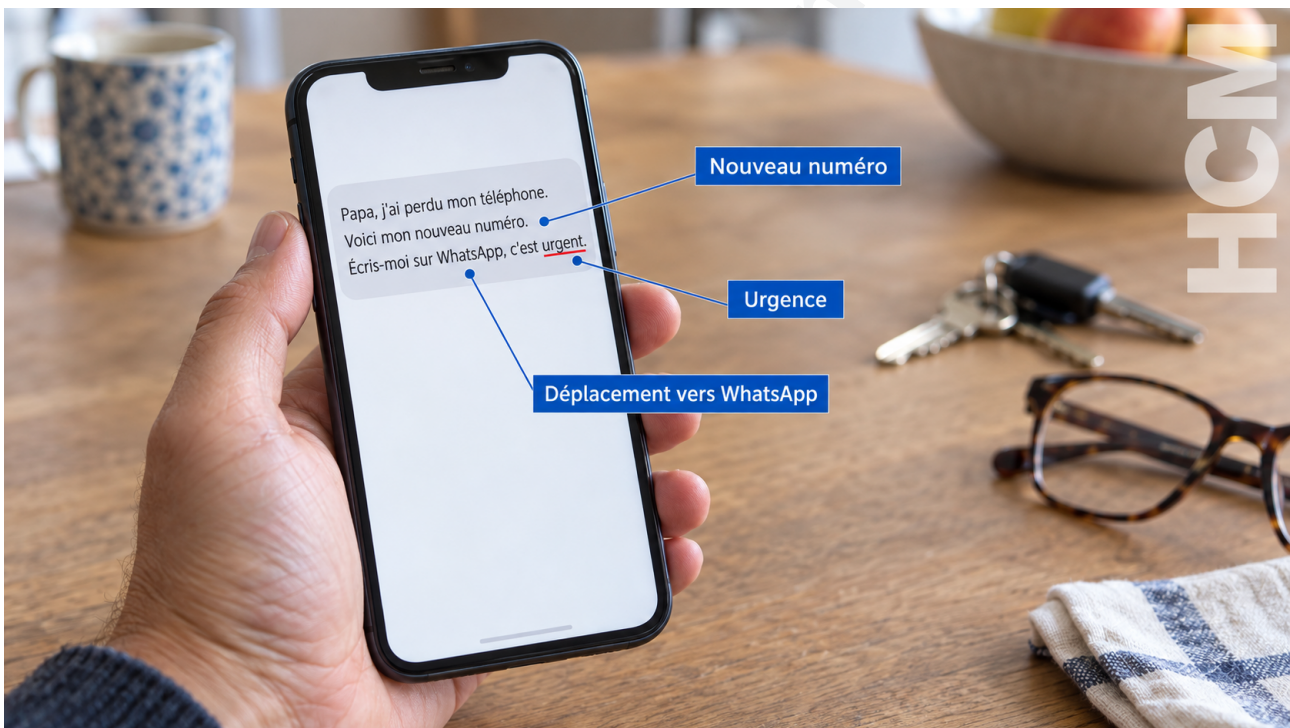
Ne répondez pas au nouveau numéro. Appelez votre enfant sur son numéro habituel. S'il ne répond pas, contactez une autre personne susceptible d'être avec lui ou utilisez un canal déjà connu. Posez si nécessaire une question dont la réponse n'est pas visible sur les réseaux sociaux.

Vous pouvez également convenir à l'avance d'un code secret entre les personnes de la famille. Il peut s'agir d'un mot inventé, d'une courte phrase absurde, d'une question avec une réponse choisie ensemble ou de toute autre formule facile à retenir, mais impossible à deviner. Ce code doit rester exclusivement privé, n'être connu que des personnes concernées et ne jamais être publié sur les réseaux sociaux. Il ne doit pas non plus être utilisé comme mot de passe pour un compte. En cas de message ou d'appel inquiétant, demandez ce code avant de croire l'identité de la personne.

Si vous avez déjà répondu ou payé

- Une simple réponse n'autorise pas l'accès à vos comptes, mais elle confirme que votre numéro est actif et que le scénario peut fonctionner. Bloquez le numéro et restez vigilant face aux relances.
- Si vous avez communiqué des données de carte, faites immédiatement opposition par le canal officiel de votre banque.
- Si vous avez effectué un virement, prévenez immédiatement la banque pour tenter de le suspendre ou de demander le retour des fonds.
- Si vous avez transmis des codes de coupons, conservez les tickets, références et messages, puis contactez sans délai l'émetteur des coupons. Une récupération n'est pas garantie.
- Conservez les preuves avant de bloquer et de signaler.

Cybermalveillance.gouv.fr recommande notamment de vérifier directement auprès de l'enfant et de signaler le SMS au 33700.



2. Le vol d'un compte WhatsApp : deux méthodes différentes

Dire " on m'a piraté WhatsApp " ne suffit pas pour comprendre l'incident. Deux scénarios très différents sont fréquents.

Méthode A : le vol du code d'enregistrement à six chiffres

Pour enregistrer un compte WhatsApp sur un téléphone, le service envoie un code par SMS ou peut proposer une vérification par appel. Le fraudeur déclenche l'enregistrement de votre numéro sur son appareil, puis invente un prétexte pour obtenir le code que vous venez de recevoir : erreur de numéro, concours, aide à un proche, vérification de sécurité, prétendu employé de WhatsApp.

S'il obtient ce code, il peut enregistrer votre compte sur son téléphone et se faire passer pour vous auprès de vos contacts. Il peut alors réclamer de l'argent, demander d'autres codes ou exploiter l'historique qui devient accessible selon les sauvegardes et les protections en place.

Le code ne lui révèle pas votre mot de passe bancaire et ne lui donne pas automatiquement accès à tout le contenu de votre téléphone. Mais il peut lui donner le contrôle de votre identité WhatsApp, ce qui suffit pour attaquer vos proches.

Méthode B : le faux QR code et l'appareil lié

WhatsApp permet de relier un ordinateur, une tablette ou un autre téléphone à un compte existant. Le fraudeur peut vous faire scanner un QR code sous prétexte de voter, de recevoir un cadeau, de rejoindre un service ou de résoudre un problème.

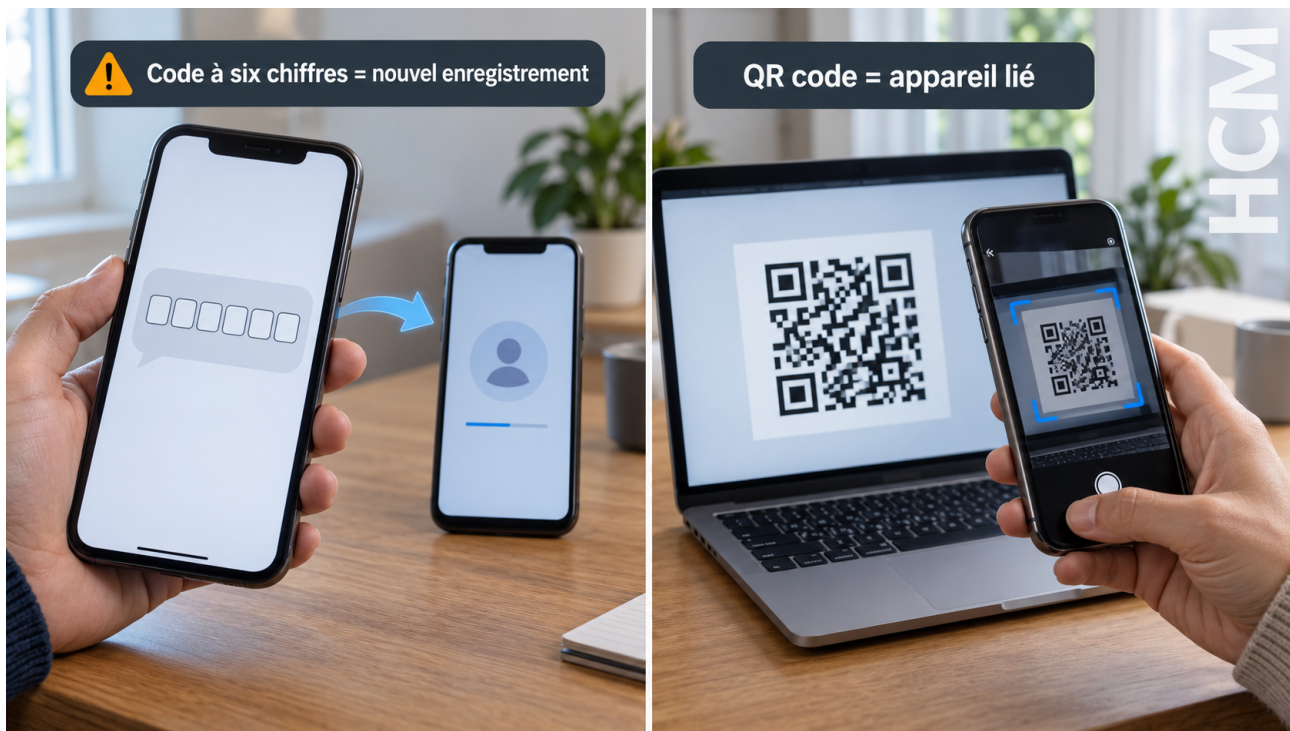
Dans ce cas, votre téléphone peut rester normalement connecté tandis qu'un appareil inconnu lit et envoie des messages depuis votre compte. Cette discrétion rend la fraude plus difficile à remarquer.

Comment vérifier et reprendre le contrôle

- Ouvrez les réglages WhatsApp et examinez la rubrique des appareils connectés ou liés.
- Déconnectez tout appareil inconnu.
- Si votre compte a été enregistré ailleurs, réenregistrez votre numéro dans l'application officielle avec le code reçu par SMS.
- Activez la vérification en deux étapes de WhatsApp et ajoutez une adresse électronique de récupération que vous contrôlez.
- Prévenez vos contacts par un autre moyen si des demandes d'argent ont été envoyées en votre nom.

Si WhatsApp fonctionne encore sur votre téléphone, ne désinstallez pas précipitamment l'application et ne vous déconnectez pas avant d'avoir vérifié les appareils liés et vos moyens de récupération.

Si votre carte SIM ne capte plus le réseau au même moment, le problème peut être un détournement de ligne : contactez d'abord l'opérateur depuis un autre téléphone.



3. Le SIM swapping : quand l'escroc détourne votre numéro

Le SIM swapping, ou échange frauduleux de carte SIM, ne consiste pas à copier toutes les données physiques de votre téléphone. L'escroc cherche à convaincre ou tromper l'opérateur pour faire attribuer votre numéro à une autre carte SIM ou eSIM qu'il contrôle.

Une fois le transfert réalisé, les appels et SMS destinés à votre numéro arrivent chez lui. Votre propre téléphone perd généralement le réseau mobile : plus d'appels, plus de SMS et souvent plus de données cellulaires, alors que le Wi-Fi peut continuer à fonctionner.

Ce que le fraudeur doit généralement posséder

Il lui faut assez d'informations pour franchir les contrôles de l'opérateur ou détourner une procédure légitime. Elles peuvent venir d'une fuite de données, d'un hameçonnage, d'un compte client opérateur compromis, de documents dérobés ou d'une manipulation d'un service d'assistance.

Le code PIN de la carte SIM protège la carte présente dans votre téléphone lorsqu'il redémarre. Il ne suffit pas à empêcher un échange frauduleux réalisé dans le système de l'opérateur.

Ce que le contrôle du numéro peut permettre

Le fraudeur peut recevoir les codes envoyés par SMS et les appels de vérification. S'il connaît déjà un identifiant ou un mot de passe, il peut tenter :

- de réinitialiser une messagerie ou un réseau social ;
- d'enregistrer WhatsApp sur son appareil ;

- d'intercepter certains codes de confirmation bancaire ;
- de modifier un moyen de récupération ;
- de valider ou préparer d'autres détournements de comptes.

Le risque vient donc souvent de la combinaison entre le numéro détourné et des informations déjà volées.

Banque, 3-D Secure et virements : ce qu'il faut comprendre

3-D Secure concerne les paiements par carte sur Internet. Selon la banque et le contexte, l'authentification peut prendre la forme d'un code SMS, d'une validation dans l'application bancaire ou d'une autre méthode forte. Certains paiements peuvent par ailleurs relever d'exemptions ou de circuits différents.

Les virements et l'ajout d'un bénéficiaire ne sont pas des opérations " 3-D Secure " : ils utilisent les mécanismes d'authentification et de validation propres à la banque. Une banque peut aussi imposer un délai, une vérification supplémentaire ou bloquer une opération jugée suspecte.

Ainsi, détourner une SIM ne garantit pas à lui seul qu'un paiement ou un virement réussira. Mais si le SMS est encore utilisé comme élément de validation ou de récupération, et si l'escroc possède aussi les identifiants nécessaires, le détournement peut contribuer à autoriser une opération, à réinitialiser l'accès bancaire ou à tenter l'enrôlement d'un nouvel appareil de confiance. Les possibilités exactes dépendent de la banque et des protections du compte.

Ce que le SIM swapping ne donne pas automatiquement

Il ne copie pas mécaniquement :

- les photos stockées uniquement dans l'appareil ;
- les fichiers locaux ;
- les mots de passe que l'escroc ne connaît pas ;
- le code de déverrouillage du téléphone ;
- ni l'accès automatique à tous les comptes bancaires.

Mais cette limite ne doit pas rassurer à tort : la messagerie électronique, les sauvegardes en ligne et les procédures de récupération peuvent ensuite ouvrir d'autres portes.

Le signal d'alerte et l'ordre des urgences

Une perte soudaine et inexpliquée du réseau, surtout si l'opérateur vous informe d'un changement de SIM ou si vous recevez auparavant des notifications de sécurité, doit être prise au sérieux.

1. Depuis un autre téléphone, contactez immédiatement l'opérateur par son numéro officiel et demandez si une nouvelle SIM ou eSIM a été activée.
2. Faites suspendre l'échange frauduleux et réattribuer la ligne.
3. Prévenez la banque si le numéro sert à confirmer des opérations ou si des mouvements apparaissent.

4. Depuis un appareil considéré comme sûr et une connexion fiable, sécurisez d'abord l'adresse électronique principale, puis les comptes importants.
5. Contrôlez les appareils connectés, les coordonnées de récupération et les opérations récentes.

Tant que l'escroc contrôle votre numéro, évitez de multiplier les demandes de codes par SMS : vous pourriez les lui envoyer. Utilisez un autre moyen de récupération lorsque le service le permet.



4. Le smishing : le SMS n'est souvent que l'appât

Le smishing est un hameçonnage transmis par SMS. Le message peut parler d'un colis, d'une amende, d'un remboursement, d'un compte bloqué, d'une facture impayée, d'une carte Vitale ou d'une opération bancaire.

Le SMS cherche généralement à provoquer l'une de ces actions : ouvrir un faux site, appeler un faux service, télécharger une application ou communiquer des informations.

Exemple concret

Vous recevez : " Votre colis ne peut pas être livré. Réglez 1,99 € avant ce soir. " Le lien ouvre un site ressemblant à celui du transporteur. Vous saisissez votre adresse et votre carte. Le faible montant sert à rendre la demande crédible ; le vrai objectif peut être de voler les données de la carte.

L'escroc peut ensuite vous appeler en se faisant passer pour la banque, puisqu'il connaît désormais vos informations. Il prétend annuler une fraude et vous demande un code ou une validation qui autorise en réalité une opération plus importante.

Un code n'est pas une formalité

Beaucoup de personnes pensent qu'un code reçu par SMS est seulement un numéro de contrôle à répéter au conseiller. C'est faux. Ce code est souvent la dernière serrure qui empêche l'escroc de terminer son opération. Si vous le lui donnez, vous pouvez lui ouvrir vous-même cette serrure.

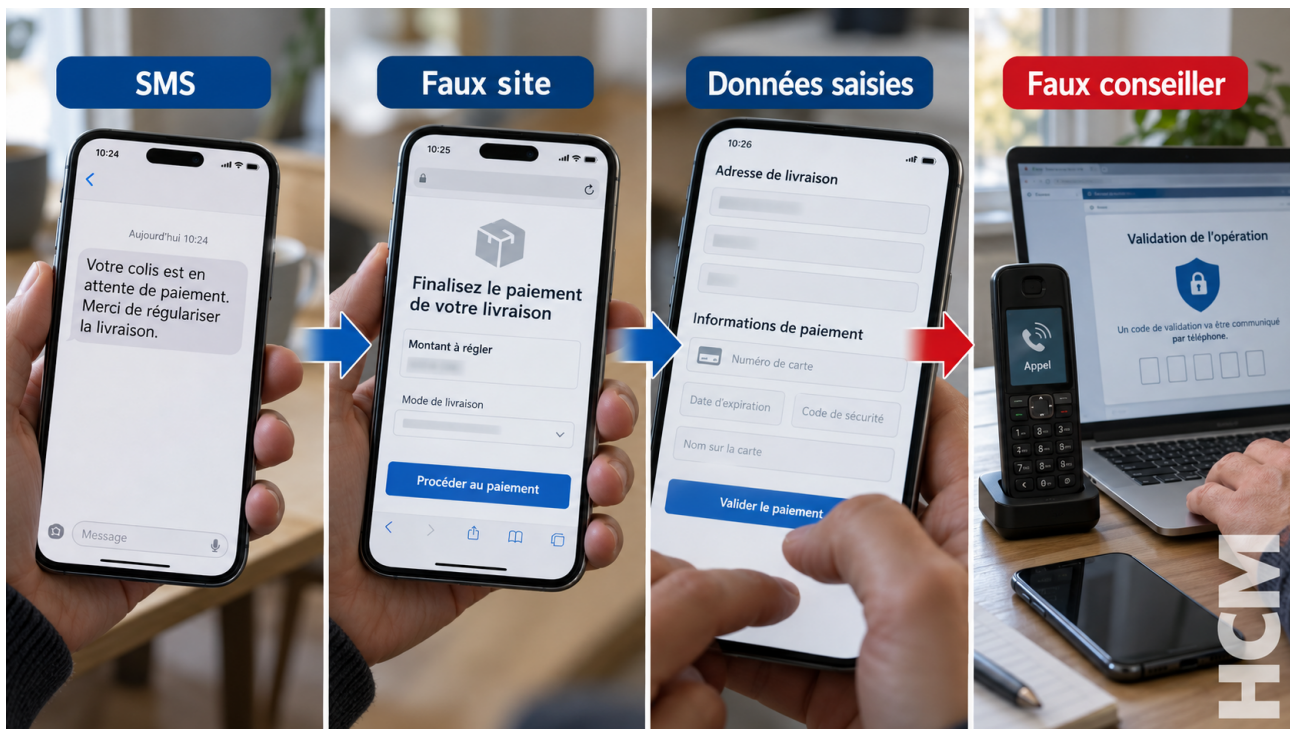
Par exemple, l'escroc possède déjà les informations de votre carte et lance un paiement de 980 €. Votre banque vous envoie alors un code pour autoriser ce paiement. Le faux conseiller prétend qu'il a besoin de ce code pour "annuler" l'opération. En réalité, s'il le saisit, le paiement peut être validé. Le même principe peut servir à autoriser une connexion, à réinitialiser un mot de passe, à ajouter un appareil ou à enregistrer une carte dans un portefeuille numérique.

Ne lisez donc jamais seulement les chiffres. Lisez entièrement le SMS ou l'écran de validation, notamment le montant, le nom du bénéficiaire, le type d'opération et l'appareil concerné. Si le message indique qu'un paiement, un virement, une connexion ou un nouvel appareil va être autorisé, le code sert à cette action, pas à l'annuler.

Le message contenant le code peut être parfaitement authentique. C'est la personne qui vous demande ce code qui ne l'est pas. Un vrai conseiller n'a pas besoin de connaître votre code de sécurité.

Que faire selon ce que vous avez fait ?

- Vous avez seulement reçu le SMS : ne cliquez pas, ne répondez pas, puis signalez-le.
- Vous avez ouvert le lien sans rien saisir ni installer : fermez la page. Un clic seul ne signifie pas automatiquement que vos comptes sont compromis, mais mettez à jour le navigateur et le téléphone et surveillez tout comportement inhabituel.
- Vous avez saisi un mot de passe : changez-le immédiatement sur le vrai site depuis un appareil sûr. Changez aussi les autres comptes où il a été réutilisé.
- Vous avez saisi les données de votre carte : contactez immédiatement la banque et suivez ses instructions, notamment pour l'opposition.
- Vous avez donné un code ou validé une demande : contactez sans attendre le service ou la banque concernée. Identifiez précisément ce que le message disait avoir autorisé.
- Vous avez installé une application ou un profil : coupez la connexion si une prise en main semble active, n'effectuez plus d'opération sensible sur l'appareil et faites-le contrôler.



5. Le faux conseiller bancaire et le numéro usurpé

L'arnaque par téléphone est appelée vishing lorsqu'elle repose sur la voix. Le spoofing désigne ici l'usurpation du numéro affiché. Un fraudeur peut donc appeler en faisant apparaître un numéro ressemblant à celui de votre banque, parfois même le véritable numéro public de celle-ci.

Le numéro affiché n'est pas une preuve d'identité.

Comment un faux numéro peut-il s'afficher ?

Lorsque vous recevez un appel, le réseau transmet la voix, mais aussi une information indiquant le numéro à afficher. Certains systèmes de téléphonie d'entreprise ou de téléphonie par Internet permettent légitimement de présenter un numéro différent de la ligne qui appelle. Par exemple, les appels passés depuis plusieurs postes d'une entreprise peuvent tous afficher le numéro de son standard.

Cette fonction doit normalement être contrôlée. Mais des fraudeurs exploitent des services ou des circuits téléphoniques, parfois situés à l'étranger, qui ne vérifient pas correctement qu'ils ont le droit d'utiliser le numéro indiqué. Ils inscrivent alors le numéro de la banque comme numéro à présenter. Votre téléphone affiche l'information qu'il reçoit, mais cela ne prouve pas que l'appel provient réellement de la ligne de la banque.

Les opérateurs mettent en place des mécanismes d'authentification pour limiter ces usurpations, mais cela ne permet pas encore de considérer chaque numéro affiché comme une preuve absolue. C'est pour cette raison qu'il faut raccrocher et rappeler soi-même la banque avec son numéro officiel. ([ABE Info Service](#) ; [ministère de l'Économie](#))

Le faux conseiller connaît parfois votre nom, votre banque, votre adresse, une partie de votre numéro de carte ou des opérations récentes. Il annonce une fraude en cours et propose de la bloquer. Puis il vous demande de lire un code, d'accepter une notification, d'ajouter un bénéficiaire, de transférer l'argent vers un prétendu " compte sécurisé " ou de remettre votre carte à un coursier.

Ce que vous croyez faire, et ce que vous faites réellement

Ce que dit l'escroc	Ce que l'action peut réellement produire
" Validez pour annuler le paiement "	Autoriser un paiement
" Acceptez pour sécuriser votre compte "	Enrôler un appareil ou confirmer une connexion
" Ajoutez ce compte technique "	Ajouter un bénéficiaire contrôlé par l'escroc
" Transférez l'argent sur un compte de sécurité "	Effectuer un véritable virement vers l'escroc
" Découpez la carte et donnez-la au coursier "	Remettre la puce et parfois le code à un complice

Une application bancaire n'affiche pas une fausse validation " inversée " destinée à annuler une fraude. Si l'écran annonce un paiement, un virement, un bénéficiaire ou un nouvel appareil, votre acceptation sert à réaliser l'action indiquée.

La seule vérification fiable

Raccrochez. Attendez quelques instants si nécessaire, puis ouvrez vous-même l'application bancaire ou composez le numéro figurant sur votre carte, votre relevé ou le site officiel saisi manuellement. Ne rappelez pas un numéro donné pendant l'appel ou dans le SMS.

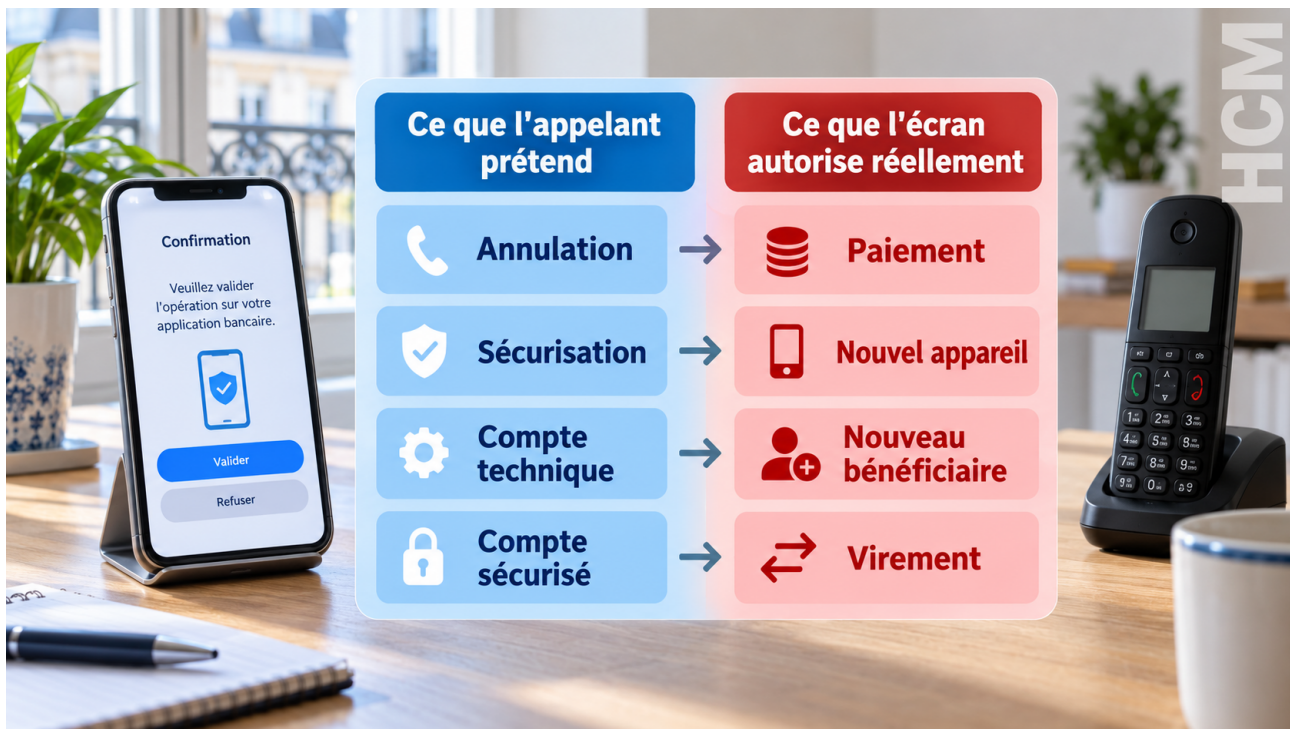
Un vrai conseiller ne vous demandera pas de lui dicter un code confidentiel, d'accepter une opération pour l'annuler, de virer vos économies sur un " compte sécurisé ", ni de confier votre carte à un coursier.

Si vous avez validé ou communiqué quelque chose

Contactez immédiatement le service de fraude ou d'opposition de la banque. Demandez le blocage des moyens de paiement concernés, la suspension d'un virement si elle est encore possible et l'examen des bénéficiaires, appareils et plafonds récemment modifiés.

Conservez les messages, numéros, heures, captures et intitulés exacts des validations.

La question d'un remboursement dépend des faits, du type d'opération et de l'examen du dossier. Il serait imprudent de promettre un remboursement automatique ou, à l'inverse, d'affirmer d'emblée qu'il est impossible.



6. Le faux support technique et la prise en main à distance

Une fenêtre surgit dans le navigateur : " Virus détecté — appelez immédiatement Microsoft/Apple ". Une voix vous appelle ensuite, ou vous composez vous-même le numéro. Le prétendu technicien vous demande d'installer un logiciel de téléassistance ou de partager l'écran.

L'alerte affichée par une page web ne prouve pas que l'appareil est infecté. Elle peut être une simple mise en scène qui bloque visuellement le navigateur, joue un son et affiche un numéro frauduleux.

Le danger commence quand l'accès est accordé

Les outils de contrôle à distance sont parfois des logiciels légitimes, utilisés par de vrais services d'assistance. Entre les mains d'un escroc, ils peuvent lui permettre de voir l'écran, déplacer le pointeur, ouvrir des fichiers, modifier des réglages, installer d'autres programmes ou observer une connexion bancaire.

Selon l'outil et sa configuration, l'accès peut cesser à la fin de la session ou rester possible ultérieurement. Désinstaller l'application de téléassistance ne prouve donc pas qu'aucun autre logiciel, compte ou réglage n'a été ajouté.

Si la session est encore active

1. Coupez immédiatement le Wi-Fi et les données mobiles, ou débranchez le câble réseau.
2. N'ouvrez plus votre banque, votre messagerie ou votre gestionnaire de mots de passe sur cet appareil.

3. Depuis un autre appareil sûr, contactez la banque si des informations financières ont été visibles ou saisies.
4. Faites contrôler l'appareil et les logiciels installés, les profils, extensions, comptes et autorisations.
5. Changez les mots de passe importants depuis un appareil sûr, en commençant par la messagerie principale.

Si vous avez seulement vu cette fausse alerte, sans appeler le numéro, sans installer de programme et sans saisir d'information, cela ne signifie pas que vos mots de passe ont été volés. Fermez complètement le programme qui vous sert à aller sur Internet, par exemple Google Chrome, Microsoft Edge, Firefox ou Safari. Si la fenêtre refuse de se fermer, redémarrez l'ordinateur ou le téléphone. À la réouverture, ne choisissez pas de restaurer les anciennes pages si le programme vous le propose.

Ensuite, effectuez les mises à jour proposées par ce programme et par l'appareil. Si la fausse alerte revient, ne cliquez pas dessus. Faites vérifier le programme de navigation afin de supprimer la page mémorisée, les autorisations de notifications douteuses et les éventuels petits modules ajoutés au programme, appelés extensions. Cette vérification peut être confiée à un professionnel si ces manipulations ne vous sont pas familières.



7. L'appel en absence qui pousse à rappeler

Le " ping call " est un appel très bref destiné à provoquer un rappel. Le coût ne vient généralement pas de la sonnerie reçue, mais du numéro surtaxé rappelé, d'une redirection ou d'une conversation volontairement prolongée.

Tous les numéros commençant par 08 ne sont pas surtaxés, et un numéro mobile français ordinaire n'est pas automatiquement payant. À l'inverse, un numéro d'apparence normale peut servir de première étape à une escroquerie ou avoir été usurpé.

Ne appelez pas par curiosité un numéro inconnu qui n'a laissé aucun message intelligible. Si le correspondant prétend représenter une entreprise ou une administration, recherchez vous-même son numéro officiel. Pour connaître le tarif d'un numéro spécial, utilisez l'annuaire prévu à cet effet sur Surmafacture.fr.

Si vous avez uniquement décroché ou rappelé brièvement sans communiquer d'information, installer d'application ni suivre d'instruction, il n'est pas nécessaire de réinitialiser le téléphone ou de changer tous vos mots de passe. Contrôlez plutôt la facture et signalez le spam vocal au 33700.

8. La voix clonée par intelligence artificielle

À partir d'enregistrements trouvés sur des vidéos, des messages vocaux ou les réseaux sociaux, des outils peuvent produire une voix ressemblant à celle d'un proche ou d'un responsable. Le fraudeur l'utilise pour annoncer un accident, une arrestation, une urgence financière ou une opération confidentielle.

Mais une voix familière ne permet pas, à elle seule, d'affirmer qu'une intelligence artificielle a été utilisée. Il peut également s'agir d'un enregistrement, d'un imitateur, d'un son dégradé ou simplement de l'effet de la panique.

Le clonage imite une voix ; il ne donne pas automatiquement accès au téléphone, aux comptes ou aux souvenirs privés de la personne. C'est pourquoi des questions contextuelles ou une vérification par un canal connu restent efficaces.

Raccrochez et appelez le proche sur son numéro habituel. Contactez une autre personne présente avec lui. Utilisez le mot de sécurité familial si vous en avez choisi un. Si une personne semble réellement en danger immédiat, contactez le 17 ou le 112 au lieu de suivre les instructions financières de l'appelant.

9. Le vol des codes de connexion et de récupération

Un code reçu de Facebook, Google, Apple, Microsoft, WhatsApp ou d'un autre service ne prouve pas que le message est frauduleux. Il peut avoir été envoyé par le véritable service parce qu'un escroc vient de tenter une connexion ou une récupération avec votre adresse ou votre numéro.

Le message peut être authentique. C'est la personne qui vous demande le code qui ne l'est pas.

La réception d'un code non sollicité ne signifie pas toujours que le compte est déjà pris. Elle peut simplement montrer que quelqu'un a lancé une tentative sans disposer du dernier élément nécessaire. Ne lui donnez pas cet élément.

Les demandes répétées de validation sont également dangereuses. Un fraudeur qui connaît déjà le mot de passe peut envoyer plusieurs notifications dans l'espoir que vous acceptiez par lassitude ou par erreur. N'approuvez jamais une connexion, une localisation ou un appareil que vous ne reconnaissez pas.

Pourquoi la messagerie électronique doit être protégée en premier

L'adresse électronique principale sert souvent à réinitialiser les autres comptes. Si un escroc la contrôle, il peut demander de nouveaux mots de passe, intercepter les alertes et effacer certains messages de sécurité. Elle constitue donc une véritable clé maîtresse.

Utilisez un mot de passe unique, activez une authentification forte qui ne dépend pas uniquement du SMS lorsque le service le permet, conservez les codes de secours hors ligne et vérifiez régulièrement les appareils connectés ainsi que les adresses ou numéros de récupération.

Si vous avez communiqué un code

Depuis une session encore ouverte ou un appareil sûr :

1. changez le mot de passe du compte concerné ;
2. vérifiez les appareils et sessions connectés ;
3. retirez les coordonnées de récupération inconnues ;
4. vérifiez les règles de transfert de courrier, applications liées et autorisations ;
5. renouvelez si nécessaire les codes de secours ;
6. sécurisez les autres comptes utilisant le même mot de passe.

Ne déconnectez pas précipitamment tous vos appareils avant d'avoir vérifié que vous possédez un autre moyen de récupération. Une session encore ouverte sur un appareil connu peut être précieuse pour reprendre le contrôle — notamment sur Facebook.

Si vous soupçonnez qu'un appareil contient un logiciel malveillant, ne saisissez pas vos nouveaux mots de passe dessus. Utilisez un appareil considéré comme sain.

FICHE RÉFLEXE

Que faire selon l'action accomplie ?

1

Message ou appel seulement reçu

Risque — manipulation ou nouvelle relance

PREMIÈRE RÉACTION Ne pas poursuivre, vérifier autrement, conserver et signaler.

2

Lien ouvert, sans saisie ni installation

Risque — exposition à un faux site

PREMIÈRE RÉACTION Fermer la page, mettre à jour l'appareil et surveiller.

3

Mot de passe saisi

Risque — prise de contrôle du compte

PREMIÈRE RÉACTION Le changer sur le vrai site et contrôler les sessions.

4

Données de la carte communiquées

Risque — paiements frauduleux

PREMIÈRE RÉACTION Contacter immédiatement la banque et suivre ses consignes.

5

Code donné ou notification acceptée

Risque — paiement, connexion ou ajout d'un appareil

PREMIÈRE RÉACTION Lire l'action autorisée et appeler le service concerné.

6

Virement effectué

Risque — départ réel des fonds

PREMIÈRE RÉACTION Appeler la banque pour tenter de suspendre le virement.

7

QR code WhatsApp scanné

Risque — appareil inconnu lié au compte

PREMIÈRE RÉACTION Examiner les appareils liés et déconnecter l'inconnu.

8

Outil de téléassistance installé

Risque — observation ou contrôle de l'appareil

PREMIÈRE RÉACTION Couper Internet et ne plus saisir d'information sensible.

9

Ligne mobile soudainement sans réseau

Risque — échange frauduleux de carte SIM

PREMIÈRE RÉACTION Appeler l'opérateur depuis une autre ligne, puis la banque.

10

Accès au compte perdu

Risque — mot de passe ou récupération modifiés

PREMIÈRE RÉACTION Utiliser la récupération officielle et garder la session ouverte.

HCM

En cas de doute, n'agissez pas dans l'urgence. Vérifiez par un autre canal.

Les protections qui réduisent réellement le risque

1. Vérifiez par un canal indépendant. Raccrochez et appelez vous-même le numéro officiel ou habituel.
2. Ne communiquez jamais un mot de passe ou un code reçu par SMS. Un service légitime ne vous demande pas de lui dicter le secret qui sert à vous authentifier.
3. Lisez chaque écran de validation jusqu'au bout. Vérifiez l'opération, le montant, le bénéficiaire et l'appareil concernés.
4. Protégez d'abord votre adresse électronique principale. Mot de passe unique, authentification forte et moyens de récupération à jour.
5. Préférez, lorsque c'est possible, une application d'authentification, une clé de sécurité ou une clé d'accès au SMS seul. Le SMS reste utile, mais dépend du contrôle de la ligne mobile.
6. Activez la vérification en deux étapes de WhatsApp et contrôlez périodiquement les appareils liés.
7. Sécurisez l'espace client de votre opérateur avec un mot de passe unique et demandez quelles protections contre les changements de SIM ou de portabilité sont proposées.
8. Installez les applications uniquement depuis les magasins officiels ou le site authentique de l'éditeur.
9. Mettez à jour le téléphone, les applications et le navigateur.
10. Préparez la crise avant qu'elle n'arrive. Conservez hors ligne les numéros officiels de la banque et de l'opérateur, les codes de secours et les informations nécessaires à la récupération.

Les erreurs à éviter pendant l'urgence

- Ne rappelez pas le numéro fourni par le message ou l'appelant pour " vérifier ". Cherchez vous-même le canal officiel.
- Ne validez jamais une opération présentée comme son annulation. Lisez ce que l'application indique réellement.
- Ne supprimez pas immédiatement les messages, journaux d'appels, reçus et captures. Ils peuvent servir à la banque, à l'opérateur et aux enquêteurs.
- Ne déconnectez pas toutes les sessions connues tant que vous n'avez pas sécurisé une voie de récupération.
- Ne changez pas vos mots de passe depuis un appareil potentiellement contrôlé à distance ou infecté.
- Ne continuez pas à demander des codes SMS si votre ligne a peut-être été détournée.
- Ne supposez pas que l'absence de débit immédiat signifie que le danger est écarté. Des données volées peuvent être réutilisées plus tard.

- Ne supposez pas non plus qu'un simple clic a forcément livré tout votre téléphone. La réponse doit être proportionnée à l'action réellement accomplie.
-

Signaler, demander de l'aide et déposer plainte

En France, plusieurs démarches existent et ne répondent pas toutes au même besoin :

- Banque et opérateur : ce sont les premiers interlocuteurs lorsqu'il faut bloquer une opération, une carte, un accès ou une ligne. Utilisez leurs coordonnées officielles.
- 33700 : signalement des SMS indésirables et spams vocaux.
- 17Cyber : diagnostic et assistance en ligne pour les victimes de cybermalveillance.
- Perceval : signalement d'une fraude à la carte bancaire lorsque les conditions du service sont remplies, notamment après opposition pour des achats en ligne non autorisés alors que la carte est toujours en votre possession.
- THESEE : signalement ou plainte en ligne pour les escroqueries sur Internet relevant de son périmètre.
- Commissariat ou brigade de gendarmerie : dépôt de plainte avec les preuves conservées.
- 17 ou 112 : uniquement en cas d'urgence immédiate ou de danger réel pour une personne.

Un signalement n'arrête pas à lui seul un paiement ni un détournement de ligne. Dans l'urgence, contactez d'abord l'organisme capable de bloquer l'action en cours : la banque, l'opérateur ou le service dont le compte a été compromis.

Conclusion : votre numéro est une clé, mais rarement la seule

Les arnaques téléphoniques modernes ne reposent pas sur une technique unique. Elles rassemblent des fragments : une donnée personnelle issue d'une fuite, un faux SMS, un appel rassurant, un numéro usurpé, un vrai code de sécurité et une validation obtenue sous pression.

Le numéro de téléphone peut être une clé d'identité, de récupération et d'authentification. Son détournement est donc sérieux. Mais comprendre les limites de chaque méthode évite deux erreurs opposées : sous-estimer un risque réel ou paniquer après une action qui n'a pas, à elle seule, compromis tout l'appareil.

Le bon réflexe tient en trois verbes : interrompre, vérifier, agir.

- Interrompre la conversation ou la manipulation.
 - Vérifier par un canal officiel choisi indépendamment.
 - Agir selon ce qui a réellement été communiqué, validé, installé ou détourné.
-

Sources et ressources officielles

- [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) — Escroquerie à l'enfant qui a un problème avec son téléphone
- [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) — Fraude au faux conseiller bancaire
- [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) — Arnaque au faux support technique
- [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) — Hameçonnage ou phishing
- [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) — Pourquoi et comment bien gérer ses mots de passe ?
- [CNIL](https://cnil.fr) — Rapport annuel 2025
- [ABE Info Service](https://abe.info-service.fr) — Spoofing, vishing, phishing et smishing
- [Ministère de l'Économie](https://ministere-economie.gouv.fr) — Arnaque au faux conseiller bancaire
- [Banque de France](https://banque-france.fr) — Prévention de la fraude sur les paiements à distance et 3-D Secure
- [WhatsApp](https://whatsapp.com) — Récupérer un compte compromis
- [WhatsApp](https://whatsapp.com) — À propos des appareils liés
- [WhatsApp](https://whatsapp.com) — Conseils de sécurité du compte
- [Apple](https://apple.com) — Reconnaître l'ingénierie sociale et les faux appels d'assistance
- [Google](https://google.com) — Sécuriser un compte piraté
- [Ma Sécurité](https://ma-securite.fr) — Les arnaques utilisant l'intelligence artificielle
- [Service-Public.fr](https://service-public.fr) — Démarchage abusif, spam vocal ou par SMS
- [33700](https://33700.fr) — Plateforme de lutte contre les spams SMS et vocaux
- [17Cyber](https://17cyber.fr) — Assistance en ligne
- [Service-Public.fr](https://service-public.fr) — Signaler une fraude à la carte bancaire avec Perceval
- [Ma Sécurité](https://ma-securite.fr) — THESEE, plainte en ligne pour les arnaques sur Internet
- [Surmafacture.fr](https://surmafacture.fr) — Tarification des numéros spéciaux

Informations et liens vérifiés le 9 septembre 2026. Les procédures exactes peuvent varier selon l'opérateur, la banque, le téléphone et le service concerné.

Christian Pelardy - Home Computer Maintenance