

JEAN LAMOUREUX

BONUS OFFERT — La Bible des Aides Retraite

GUIDE **ANTI-ARNAQUES** **SENIORS**

Comment reconnaître et éviter les pièges financiers qui ciblent les retraités

Pourquoi les retraités sont-ils les premières cibles ?

Ce n'est pas un hasard. Plus de 70 % des arnaques signalées en France ciblent des personnes de plus de 60 ans. Les escrocs le savent : les retraités ont souvent des économies accumulées sur toute une vie de travail, reçoivent des virements réguliers et prévisibles, font davantage confiance aux interlocuteurs qui semblent officiels, et sont moins familiers des nouvelles techniques de manipulation numérique.

La bonne nouvelle : une fois que vous connaissez les 3 signaux d'alerte universels et les arnaques les plus courantes, vous êtes protégé. Parce que presque toutes les arnaques — même les plus sophistiquées — utilisent exactement les mêmes mécanismes psychologiques.

Ce guide vous donne les outils pour les reconnaître et les neutraliser immédiatement.

LES 10 ARNAQUES LES PLUS COURANTES EN 2026

Arnaque 1 — Le faux conseiller retraite

Le scénario : un homme ou une femme vous appelle en se présentant comme « conseiller retraite indépendant », « expert en droits seniors » ou « auditeur de pension ». Il vous propose un bilan gratuit de votre situation retraite. Lors du rendez-vous (parfois à domicile, parfois par téléphone), il découvre de nombreuses « anomalies » dans votre dossier et des droits non réclamés. Pour les récupérer, il vous propose ses services moyennant des honoraires de 200 à 1 500 euros. Parfois, il vous demande une procuration pour agir en votre nom.

Ce qu'il faut savoir : ces démarches peuvent être faites gratuitement, directement auprès de votre caisse de retraite, de la CAF ou des impôts. Aucun intermédiaire n'est nécessaire. Et la procuration est particulièrement dangereuse : elle peut être utilisée pour accéder à vos comptes.

 **Ne signez jamais de procuration sans en parler d'abord à un proche de confiance ou à votre banquier.**

Arnaque 2 — Le faux remboursement d'impôts

Le scénario : vous recevez un SMS ou un email vous informant qu'un remboursement d'impôts vous attend. Il suffit de cliquer sur un lien et de renseigner vos coordonnées bancaires pour recevoir la somme dans les 48 heures.

La réalité : les remboursements d'impôts légitimes arrivent directement sur le compte bancaire que vous avez déclaré à l'administration fiscale, sans aucune action de votre part. L'administration fiscale ne vous contacte jamais par SMS pour un remboursement.

✓ Si vous pensez avoir droit à un remboursement fiscal, connectez-vous vous-même sur impots.gouv.fr et vérifiez votre espace personnel.

Arnaque 3 — Le démarchage aux travaux « 100 % financés par l'État »

Le scénario : un individu sonne à votre porte et vous propose des travaux de rénovation énergétique (isolation, pompe à chaleur, panneaux solaires) « entièrement financés par l'État ». Il vous presse de signer un bon de commande « pour réserver le prix ». Les travaux sont mal réalisés, surfacturés, ou ne sont jamais effectués. Parfois, l'escroc vous fait signer un contrat de crédit à la consommation sans que vous en preniez conscience.

Ce qu'il faut savoir : les vraies aides publiques comme MaPrimeAdapt' ou MaPrimeRénov' ne sont jamais démarchées à domicile. Vous devez vous-même déposer une demande en ligne sur le site officiel de l'ANAH, et l'accord doit être obtenu AVANT de signer le moindre devis avec un artisan.

⚠ Ne signez jamais un bon de commande lors d'un démarchage à domicile lors d'une première visite.

Arnaque 4 — La fausse mutuelle ou complémentaire santé

Le scénario : vous recevez un appel d'un « conseiller en protection sociale » qui vous propose une mutuelle « spéciale seniors », « remboursée à 100 % par la Sécurité Sociale » ou « prise en charge par l'État ». Le conseiller connaît parfois vos informations personnelles, ce qui renforce votre confiance. Vous signez un contrat. Des prélèvements commencent sur votre compte. La mutuelle ne couvre rien ou très peu.

Ce qu'il faut savoir : la seule mutuelle réellement gratuite sous conditions de revenus est la Complémentaire Santé Solidaire (CSS), accessible uniquement via ameli.fr ou votre CPAM. Elle ne se négocie pas par téléphone avec des commerciaux.

✓ Si quelqu'un vous propose une mutuelle gratuite par téléphone, raccrochez. Appelez ensuite votre CPAM au 3646 pour vérifier votre éligibilité à la vraie CSS.

Arnaque 5 — L'arnaque au placement senior « garanti »

Le scénario : un « conseiller en gestion de patrimoine » vous contacte pour vous proposer un placement présenté comme sûr, à rendement élevé (8 %, 12 %, parfois plus), « réservé aux seniors » ou « spécial retraités ». Il peut s'agir de faux placements immobiliers, de crypto-monnaies, de produits financiers exotiques ou de schémas de type pyramidal. Vous investissez. Vous ne récupérez rien, ou seulement au début pour vous inciter à investir davantage.

La règle à retenir : un placement légal et sûr rapporte en 2026 entre 2 % et 4 % par an. Tout rendement supérieur à 5 % annoncé comme « garanti » est soit à risque très élevé, soit frauduleux.

 Avant tout investissement, vérifiez sur registre.abi-infoservice.fr que l'entreprise est bien autorisée par l'AMF (Autorité des Marchés Financiers).

Arnaque 6 — La fraude au compte bancaire par téléphone

Le scénario : vous recevez un appel d'un « conseiller de votre banque » vous alertant d'une transaction suspecte sur votre compte. Pour « sécuriser » vos fonds, il vous demande de valider une opération avec votre code de confirmation reçu par SMS, de virer votre argent sur un « compte sécurisé temporaire », ou de lui communiquer vos identifiants bancaires.

Ce n'est jamais votre banque. C'est un escroc qui a usurpé le numéro de téléphone de votre banque (une technique appelée « spoofing »).

La règle absolue : votre banque ne vous demandera jamais de communiquer un code reçu par SMS, ni de virer de l'argent par téléphone. Si vous avez un doute, raccrochez et appelez votre banque en composant vous-même le numéro au dos de votre carte bancaire.

Arnaque 7 — L'arnaque à l'héritage ou au gain inattendu

Le scénario : vous recevez un email, une lettre ou un message vous informant que vous êtes bénéficiaire d'un héritage d'un parent éloigné à l'étranger, ou gagnant d'une loterie à laquelle vous n'avez pas participé. Pour débloquer la somme, il faut payer des « frais administratifs » ou des « taxes de déblocage ». Ces frais augmentent à chaque étape, et l'argent promis n'arrive jamais.

 Règle simple : aucun gain ou héritage légitime ne nécessite de payer des frais à l'avance pour être débloqué. Jamais.

Arnaque 8 — Le faux support informatique

Le scénario : une fenêtre pop-up apparaît sur votre ordinateur avec un message alarmant (« Votre ordinateur est infecté ! Appelez immédiatement le numéro d'urgence »). Vous appelez. Un « technicien » vous demande l'autorisation d'accéder à distance à votre ordinateur pour « nettoyer le virus ». Une fois connecté, il accède à vos fichiers, vos mots de passe, et parfois à votre interface bancaire en ligne.

Ce qu'il faut savoir : Microsoft, Apple, et les éditeurs d'antivirus ne prennent jamais contact avec vous spontanément. Si vous voyez ce type de message, fermez simplement la fenêtre ou redémarrez votre ordinateur.

✓ Si vous avez accidentellement donné accès à votre ordinateur, changez immédiatement tous vos mots de passe depuis un autre appareil et appelez votre banque.

Arnaque 9 — La fraude à la carte bancaire en magasin

Le scénario : en payant en magasin, dans un distributeur automatique, ou lors d'un achat en ligne, vos informations de carte bancaire sont copiées (on parle de « skimming »). Des achats sont ensuite effectués sans votre accord.

Comment se protéger : couvrez toujours votre main quand vous tapez votre code. Vérifiez régulièrement votre relevé de compte (au moins une fois par semaine). Signalez immédiatement tout débit inconnu à votre banque.

aire plutôt que par virement (contestations plus faciles en cas de fraude).

7 RÉFLEXES NUMÉRIQUES QUI VOUS PROTÈGENT

1. Créez des mots de passe différents pour chaque site important (banque, impôts, ameli). Utilisez au minimum 8 caractères avec majuscules, chiffres et symboles.
2. Activez la double authentification sur votre compte bancaire en ligne et votre email. Cela signifie qu'en plus du mot de passe, un code vous est envoyé par SMS pour confirmer chaque connexion.
3. Vérifiez régulièrement votre relevé bancaire en ligne. Idéalement une fois par semaine.
4. Ne communiquez jamais votre mot de passe ou votre code PIN à qui que ce soit, même à quelqu'un qui prétend être votre banque.
5. Méfiez-vous des Wi-Fi publics (cafés, aéroports, hôtels). N'accédez pas à vos comptes bancaires sur ces réseaux.
6. Installez les mises à jour de votre téléphone et ordinateur régulièrement. Elles corrigent souvent des failles de sécurité.
7. Si vous recevez un message urgent de la part d'un proche (« j'ai un accident, envoie-moi de l'argent »), appelez cette personne directement avant d'agir.