



FICHE D'INFORMATION N°2

Sécurité & Arnaques

Comment se protéger ?

Les arnaques ciblent souvent les seniors. Cette fiche vous aide à les reconnaître et à vous en protéger.

Chaque année en Suisse, des milliers de personnes se font escroquer par téléphone, email ou SMS. Les seniors sont particulièrement visés — non pas parce qu'ils sont naïfs, mais parce que les escrocs sont très professionnels. Connaître leurs méthodes, c'est déjà se protéger à moitié.

! Les arnaques les plus courantes



Le faux support informatique

● TRÈS RÉPANDU EN SUISSE

Vous recevez un appel d'une personne se présentant comme un technicien de **Microsoft, Apple ou Swisscom**. Elle vous dit que votre ordinateur est infecté par un virus et qu'elle doit y accéder à distance pour le réparer.

💬 Ce qu'ils disent : "Bonjour, je vous appelle de Microsoft. Nous avons détecté un virus sur votre ordinateur. Je dois prendre le contrôle de votre appareil pour vous aider."

✓ **Microsoft, Apple et Swisscom ne vous appelleront JAMAIS spontanément.**

Raccrochez immédiatement. Ne donnez jamais accès à votre ordinateur à un inconnu.



Le faux employé de banque

● EN FORTE AUGMENTATION

Quelqu'un se présente comme un employé de votre banque et vous dit que votre compte a été piraté. Il vous demande vos codes, mots de passe, ou de transférer de l'argent sur un "compte sécurisé".

💬 *Ce qu'ils disent : "Bonjour, je suis de la PostFinance. Votre compte est en danger. Pour le protéger, j'ai besoin de votre code SMS maintenant."*

✓ **Votre banque ne vous demandera JAMAIS votre code SMS ni votre mot de passe.**

Raccrochez et appelez directement votre banque au numéro au dos de votre carte.



Le faux SMS de livraison

● TRÈS FRÉQUENT PAR SMS ET EMAIL

Vous recevez un SMS ou email indiquant qu'un colis vous attend et qu'il faut payer des frais de douane ou cliquer sur un lien pour confirmer la livraison.

💬 *Ce qu'ils écrivent : "Votre colis N°CH8492 est en attente. Payez 2.50 CHF de frais de livraison ici : [lien suspect]"*

✓ **Ne cliquez jamais sur un lien reçu par SMS.**

Si vous attendez un colis, allez directement sur le site de La Poste ou DHL en tapant l'adresse vous-même.



L'arnaque sentimentale ("Romance scam")

● SOUVENT TRÈS DIFFICILE À DÉTECTER

Une personne vous contacte sur les réseaux sociaux ou par email. Elle est charmante, attentionnée, dit tomber amoureux/se. Après quelques semaines, elle vous demande de l'argent pour une urgence.

💬 *Ce qu'ils disent : "Je dois rentrer de mission au plus vite pour vous voir, mais j'ai besoin de 500 CHF pour le billet. Je vous rembourserai dès mon arrivée."*

✓ **Ne transférez jamais d'argent à quelqu'un que vous n'avez jamais rencontré en personne.**

Parlez-en à un proche de confiance avant toute décision.



Le faux gain / loterie

● CLASSIQUE MAIS ENCORE EFFICACE

Vous recevez un message vous annonçant que vous avez gagné un prix (voiture, voyage, somme d'argent). Pour le recevoir, on vous demande de payer des "frais administratifs".

💬 *Ce qu'ils écrivent : "Félicitations ! Vous avez été sélectionné pour gagner 15'000 CHF. Pour recevoir votre gain, veuillez régler 50 CHF de frais de traitement."*



On ne paie jamais pour recevoir un gain.

Si vous n'avez pas participé à un concours, vous ne pouvez pas en avoir gagné un. Ignorez et supprimez.



Les 6 règles d'or SeniorPhone

1

Ne communiquez jamais vos mots de passe ou codes à personne

Ni par téléphone, ni par email, ni par SMS — jamais, à personne, sous aucun prétexte.

2

Ne cliquez jamais sur un lien reçu par SMS

Tapez toujours l'adresse du site vous-même dans votre navigateur.

3

En cas de doute, raccrochez et appelez vous-même

Utilisez le numéro officiel au dos de votre carte bancaire ou sur le site officiel.

4

Ne transférez jamais d'argent sous pression

Les vrais urgences financières se vérifient. Prenez le temps de réfléchir et d'en parler à un proche.

5

Ne donnez jamais accès à votre ordinateur à un inconnu

Microsoft, Apple et Swisscom ne vous appellent jamais spontanément pour vous aider.

6

Parlez-en à un proche avant d'agir

Un regard extérieur permet souvent de détecter une arnaque que l'on n'a pas vue.

Que faire en cas d'appel suspect ?

Numéro masqué

Votre écran affiche "*Numéro privé*" ou "*No. inconnu*" — la personne cache volontairement son identité.

Ne répondez pas. Raccrochez.

? Numéro inconnu

Vous ne reconnaissez pas le numéro. Laissez sonner. Si c'est important, la personne laissera un message vocal.

Attendez. Appelez si message.

 **Attention aux numéros 0900** — ce sont des numéros surtaxés qui vous coûtent plusieurs francs par minute. Ne rappelez jamais un numéro commençant par **0900** si vous ne savez pas à qui il appartient.

Arnaque en forte hausse en Suisse : Faux policier / Faux banquier

La Police Cantonale Vaudoise alerte sur cette arnaque qui touche principalement les personnes âgées. Des escrocs appellent en se faisant passer pour un policier ou un employé de banque.

Ce qu'ils disent :

"Je suis l'inspecteur Dupont de la police, votre compte bancaire est en danger. Nous avons besoin de votre argent pour une enquête — remettez vos billets à notre agent."

Autre variante :

"Je suis de votre banque, des malfaiteurs ont accès à votre compte. Donnez-nous votre code PIN ou transférez votre argent sur ce compte sécurisé."

 **La règle absolue :** La vraie police et votre vraie banque ne vous demanderont **JAMAIS** de remettre de l'argent en espèces, de donner votre code PIN ou de transférer des fonds par téléphone.

Si cela vous arrive — raccrochez immédiatement et appelez le

 **117**

Police — numéro d'urgence suisse

Ce qu'il faut retenir

- Les arnaques par téléphone, SMS et email sont très professionnelles — ce n'est pas une question de naïveté.
- Ni votre banque, ni Microsoft, ni Swisscom ne vous demanderont jamais vos codes.
- En cas de doute : raccrochez, réfléchissez, appelez un proche.
- Ne cliquez jamais sur un lien reçu par SMS, même s'il semble officiel.
- Vous pouvez signaler une arnaque à la police cantonale ou sur cybercrime.ch



Alerte signalée par la Police cantonale de Genève — juin 2026

Des escrocs distribuent dans les boîtes aux lettres de **faux avis de passage** imitant parfaitement ceux de La Poste Suisse. Le document est extrêmement crédible et difficile à distinguer de l'original.



Comment fonctionne cette arnaque :

- 1 Vous recevez un faux "Avis de passage" La Poste dans votre boîte aux lettres
- 2 Il vous invite à scanner un QR code pour "reprogrammer votre livraison"
- 3 Le QR code mène vers un **faux site** qui ressemble exactement à celui de La Poste
- 4 On vous demande vos coordonnées et un paiement de CHF 2.10 de "frais"
- 5 **But réel : voler les données de votre carte bancaire !**



Les règles à retenir absolument :

- **La Poste Suisse ne demande JAMAIS de paiement par QR code** pour une livraison
- **Ne scannez jamais un QR code** reçu dans votre boîte aux lettres sans vérifier
- En cas de doute — appelez directement La Poste au **0800 888 888** (gratuit)
- Le vrai site de La Poste est toujours **post.ch** — vérifiez l'adresse



Si vous avez scanné le QR code et payé : Contactez immédiatement votre banque pour signaler la fraude et faites bloquer votre carte bancaire.

Numéros et ressources utiles en Suisse

 Police (urgences)

117

 Signaler une cybercriminalité

cybercrime.ch

 Liste Robinson (stop démarchage)

robinson.ch

 En cas de fraude bancaire

Appelez votre banque immédiatement

 Alertes arnaques en Suisse

fedpol.admin.ch

Ce mois-ci, SeniorPhone est soutenu par :

[Espace réservé au sponsor du mois]

Un seul sponsor par mois — pour garder votre confiance.

Sécurité — À retenir absolument

 **Ne communiquez jamais vos mots de passe ou codes à qui que ce soit**

Ni par téléphone, ni par email, ni par SMS. Ni votre banque, ni la police, ni un opérateur ne vous les demanderont jamais.

 **Appel masqué — ne pas répondre**

Un numéro masqué cache volontairement son identité. Raccrochez sans hésiter.

 **Numéro inconnu — évitez de répondre**

Laissez sonner, attendez un message vocal, rappelez uniquement si nécessaire. Ne rappelez jamais un numéro 0900.

 **Faux policier ou faux banquier — raccrochez et appelez le 117**

La vraie police et votre banque ne vous demanderont JAMAIS de remettre de l'argent ou votre code PIN par téléphone.

Ce bandeau apparaît sur chaque fiche SeniorPhone — parce que votre sécurité est notre priorité absolue.

SeniorPhone — L'information numérique simple et honnête pour les seniors

 Pour recevoir cette fiche par email : inscrivez-vous gratuitement sur seniorphone.ch

