



En toute sécurité au quotidien

Comment se protéger contre les abus financiers ?

Se protéger contre les abus financiers

La Suisse est un pays sûr. Pendant la vieillesse également, on peut se sentir en sécurité chez soi, se déplacer et mener sa vie en toute quiétude, sans avoir peur.

Toutefois, de nouvelles arnaques financières sont continuellement inventées. Souvent, on en est victime au moment où l'on s'y attend le moins, comme en répondant au téléphone, à des SMS et à des e-mails ou en ouvrant à quelqu'un qui sonne à la porte.

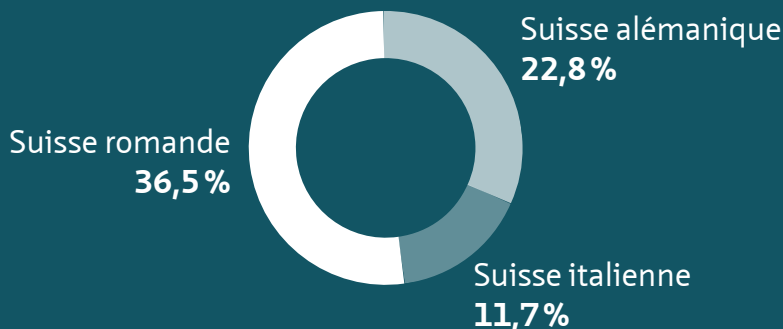
Nous vous donnons ici des conseils pour vous protéger de divers abus financiers. Pour continuer à vivre en toute sécurité, gardez l'œil ouvert !

Faits et chiffres

Sur mandat de Pro Senectute, l'Institut de lutte contre la criminalité économique (ILCE) de la Haute école de gestion Arc à Neuchâtel (HEG Arc) a étudié l'ampleur du phénomène des abus financiers chez les personnes de 55 ans et plus en Suisse.

690 335 personnes

de 55 ans et plus auraient été victimes d'un abus financier au cours des cinq dernières années.



Les hommes (**28,2%**) seraient davantage victimes d'abus financiers que les femmes (**23,3%**).

Vous trouverez davantage de résultats sur notre site prosenectute.ch/abus-financiers

La sécurité numérique

Internet, les smartphones et les e-mails font partie de notre quotidien. L'e- banking et les réseaux sociaux rencontrent aussi un grand succès. Or, l'univers numérique ouvre la porte à de nouveaux types d'escroqueries.

L'hameçonnage (phishing), par exemple, consiste à dérober des données confidentielles aux internautes.

Les fausses annonces de vente en ligne sont très fréquentes. Il faut être vigilant et se méfier des trop bonnes affaires.

Les rançongiciels (ransomware) sont des logiciels malveillants qui bloquent l'accès aux données et demandent le paiement d'une rançon pour leur déblocage. Pour s'en prémunir, il faut faire attention aux éléments téléchargés sur le web ou encore dans les pièces jointes des e-mails. Dans tous les cas, il ne faut pas payer la rançon, mais prendre contact avec les autorités locales.

Bon à savoir



Un mot de passe efficace contient au moins 12 signes, dont des majuscules, des minuscules, des chiffres et des caractères spéciaux.

Conseils de sécurité numérique :

● Ne transmettez pas vos données d'accès (identifiant et mot de passe).

● Choisissez un mot de passe sûr et n'utilisez pas le même mot de passe pour tous vos comptes. Pensez à les modifier régulièrement et conservez-les dans un endroit indépendant de votre ordinateur.

● Gardez un regard critique sur les e-mails, SMS et WhatsApp. Les apparences sont parfois trompeuses. N'ouvrez jamais de pièce jointe provenant d'un expéditeur inconnu et ne cliquez sur aucun lien.

● Méfiez-vous des demandes de données personnelles par e-mail, SMS et WhatsApp.

● Installez régulièrement les mises à jour de vos programmes et applications ; idéalement, utilisez la fonction automatique de mise à jour. Veillez à installer uniquement les mises à jour officielles.

● Protégez vos appareils au moyen d'un logiciel antivirus et d'un pare-feu, en veillant à ce que celui-ci soit bien activé.

● Réglez les paramètres de sécurité sur les réseaux sociaux, de sorte que seules les informations que vous souhaitez soient publiques.

● Veillez à ce que les sites d'achat en ligne contiennent « https:// » dans l'adresse. Le « s » de « https » prouve que le site est bien sécurisé. Mais prudence, le « s » ne signifie toutefois pas que le site est fiable.

Arnaques au téléphone et à domicile

Recevoir un appel d'une vieille connaissance fait toujours plaisir et les escrocs le savent. Ils se font donc passer pour des proches, des amis et parfois même pour des policiers pour soutirer de l'argent. Il n'est pas rare qu'ils essaient par exemple de vendre du vin ou des produits de santé. Des tentatives d'arnaques semblables se produisent également à domicile.

Parfois, des escrocs se font passer pour des employés d'un service de soutien informatique et demandent de l'argent pour aider à résoudre des soi-disant problèmes.

Bon à savoir



Les numéros de téléphone affichés peuvent être falsifiés. Il est donc tout à fait possible que derrière un numéro suisse, voire le numéro d'urgence de la police 117, se cache un appel en provenance de l'étranger.

Conseils :

Faites preuve de méfiance : si une personne qui vous téléphone vous fait deviner qui elle est, la vigilance est de mise.

Ne cédez pas à la pression : ne transmettez jamais par téléphone des données personnelles et n'acceptez pas de demande d'argent.

En cas de doute, raccrochez. Cela n'est pas impoli ; il en va de votre sécurité.

Inscrivez uniquement l'initiale de votre prénom dans l'annuaire téléphonique. Les escrocs recherchent souvent des prénoms traditionnels.

Méfiez-vous du démarchage à domicile : informez-vous préalablement du prix et procurez-vous une autre offre à titre de comparaison.

Demandez de l'aide : contactez votre entourage ou communiquez à la police vos doutes éventuels.

Faites valoir vos droits : si vous avez conclu un contrat par téléphone et que vous changez d'avis, vous disposez de 14 jours pour le résilier.

Ne payez pas des produits que vous n'avez pas commandés. Une pratique consiste en effet à envoyer des produits non commandés, puis à les facturer.

Vols

Les vols à l'astuce ne se produisent pas uniquement pendant les vacances. En Suisse aussi, les voleurs utilisent des techniques astucieuses, comme demander de l'aide, pour déconcentrer leur victime. Les pickpockets sévissent surtout dans les endroits très fréquentés, comme les gares ou les transports publics.

Bon à savoir



Portez votre sac du côté opposé au trafic et gardez vos valeurs dans les poches intérieures de vos vêtements.

Conseils :

Évitez d'avoir de grandes quantités d'argent liquide sur vous.

● Ne vous laissez pas distraire lorsque vous retirez de l'argent au bancomat.

● Faites preuve de vigilance si quelqu'un vous bouscule ou vous demande un renseignement.

● Lorsque vous payez avec une carte, veillez à ce que personne ne puisse lire votre code PIN.

● Vérifiez minutieusement vos extraits de comptes et vos décomptes de cartes de crédit. Si une transaction vous semble suspecte, prenez rapidement contact avec votre banque.

● Ne laissez pas entrer un inconnu chez vous, même si cette personne semble digne de confiance et est bien habillée. Les escrocs portent aussi des costumes et des cravates...

Que faire en cas d'abus financier ?

Les escrocs ont souvent un temps d'avance sur nous. Malgré toutes les précautions du monde, il n'est donc pas impossible d'être un jour victime d'un abus financier. Si tel est le cas, ne perdez pas de temps et agissez immédiatement :

- **Contactez la police** : en cas d'urgence, composez le 117 ou, pour les cas moins urgents, contactez le poste de police le plus proche.
- **Bloquez sans attendre vos comptes et vos cartes** en cas de vol ou de perte.
- **Modifiez votre mot de passe ou votre code PIN** si vous avez le sentiment que quelqu'un connaît vos données d'accès.
- **Parlez-en** : informez vos proches et vos amis pour leur éviter la même mésaventure.
- **Faites-vous conseiller** : vous trouverez auprès de la police des spécialistes qui répondront volontiers à vos questions en matière de sécurité.

Pro Senectute, la police et d'autres organisations proposent régulièrement des séances d'information ou des formations sur le thème de la sécurité. L'Institut de lutte contre la criminalité économique (ILCE) dispense également des formations en matière de cybercriminalité. Par ailleurs, n'hésitez pas à partager vos expériences et vos connaissances.

La Prévention Suisse de la Criminalité propose des informations détaillées sur la criminalité : skppsc.ch/fr

Vous trouverez davantage d'informations et des adresses utiles sur notre site prosenectute.ch/abus-financiers ou auprès d'un bureau de consultation Pro Senectute près de chez vous.

Pro Senectute Suisse
Secrétariat romand
Rue du Simplon 23
1800 Vevey
Téléphone 021 925 70 10

info@prosenectute.ch
prosenectute.ch