

La lettre de l'assistante sociale

Votre service social vous informe au 09 80 80 03 07

PRESTASOCIAL

COMMENT LE SERVICE SOCIAL DU TRAVAIL PEUT VOUS SOUTENIR?

En toute confidentialité, votre assistante sociale vous écoute, vous informe, vous accompagne dans les démarches et vous soutient dans toutes les étapes de votre vie professionnelle et privée.



Un message de prévention important

Les escroqueries peuvent concerner tout le monde, quel que soit l'âge, la profession ou le niveau de connaissance en informatique. Les fraudeurs savent parfaitement créer un climat de confiance ou de panique pour pousser leurs victimes à agir rapidement sans prendre le temps de vérifier.

La meilleure protection reste la vigilance, l'échange d'informations et la prévention.

Parler des arnaques autour de soi permet aussi de protéger ses proches.

FRAUDES ET ARNAQUES

SOYONS VIGILANTS, PROTÉGEONS-NOUS !



NE DONNEZ JAMAIS vos informations personnelles ou bancaires.



MÉFIEZ-VOUS des messages ou appels inattendus.



VÉRIFIEZ TOUJOURS l'expéditeur et le site internet avant de cliquer.



EN CAS DE DOUTE, parlez-en à un proche ou contactez un professionnel.



La meilleure défense, c'est votre vigilance !



Victime ou témoin d'une fraude ?
Contactez le 17 ou le 0 805 805 817
Service & appel gratuits

FRAUDES, ARNAQUES ET USURPATION D'IDENTITÉ: COMMENT SE PROTÉGER D'UN PHÉNOMÈNE EN FORTE AUGMENTATION?

Les fraudes et les arnaques ne concernent plus seulement quelques situations isolées. Aujourd'hui, chacun peut être confronté à une tentative d'escroquerie, que ce soit par téléphone, par SMS, par e-mail, sur internet ou même directement à domicile.

Les méthodes utilisées par les fraudeurs évoluent sans cesse. Certains se font passer pour des banques, des administrations ou des entreprises connues afin de gagner la confiance de leurs victimes. D'autres utilisent les réseaux sociaux, les sites de vente en ligne ou les applications de messagerie pour récupérer de l'argent ou des informations personnelles.

Chaque année, des milliers de personnes perdent de l'argent à la suite d'une escroquerie. Mais au-delà des pertes financières, certaines victimes doivent également faire face à des difficultés administratives, à des démarches longues et parfois à un véritable sentiment d'insécurité après une usurpation d'identité.

Même les personnes prudentes peuvent être piégées. C'est pourquoi l'information et la prévention sont essentielles pour apprendre à reconnaître les situations à risque et adopter les bons réflexes.

1/ LES ARNAQUES LES PLUS FRÉQUENTES:



Les faux appels bancaires:

Cette arnaque est devenue très fréquente. Un fraudeur appelle en prétendant travailler pour votre banque. Son discours est souvent rassurant et très convaincant.

Il explique généralement qu'une opération suspecte serait en cours sur votre compte et tente ensuite de vous pousser à :

- communiquer vos codes bancaires ;
- valider une opération sur votre téléphone ;
- transférer votre argent vers un « compte sécurisé ».



Peut-on être victime même en étant prudent ?

Oui. Les escrocs utilisent des méthodes de plus en plus convaincantes et professionnelles. Tout le monde peut être concerné.

L'important est de réagir rapidement et de demander de l'aide en cas de doute.



Que faire si j'ai cliqué sur un lien suspect ?

- ✓ ne saisissez plus aucune information ;
- ✓ changez rapidement vos mots de passe ;
- ✓ contactez votre banque si des données bancaires ont été communiquées ;
- ✓ effectuez un scan antivirus de votre appareil.



Est-il dangereux d'envoyer une copie de sa carte d'identité ?

Oui, si cela est fait sans précaution.

Ajoutez toujours une mention indiquant la raison de l'envoi et le destinataire, afin de limiter les risques de réutilisation



Faut-il porter plainte en cas d'arnaque ?

Oui. Même si le montant paraît faible, le dépôt de plainte permet :

- ✓ de signaler les faits ;
- ✓ d'aider les enquêtes ;
- ✓ de protéger d'autres victimes ;
- ✓ de disposer d'une preuve auprès des banques ou assurances.

Une banque ne demande jamais :

- ✓ vos codes confidentiels ;
- ✓ un mot de passe complet ;
- ✓ de transférer votre argent par téléphone.

En cas de doute, raccrochez et contactez directement votre banque avec le numéro officiel figurant sur vos documents.

✓ Les SMS et e-mails frauduleux (phishing) :

Cette technique, appelée « phishing », consiste à envoyer un message semblant provenir d'un organisme officiel : banque, impôts, assurance maladie, service de livraison ou opérateur téléphonique.

Le message demande généralement de cliquer sur un lien pour confirmer une information, payer un montant, débloquer un colis, éviter une sanction...

Une fois sur le faux site, vos informations personnelles ou bancaires sont récupérées.

Plusieurs signes doivent alerter : des fautes d'orthographe, une adresse e-mail étrange, un sentiment d'urgence, une menace de blocage ou un lien internet inhabituel.

Ne cliquez jamais dans la précipitation.

✓ Les arnaques aux achats en ligne :

Certains faux sites internet proposent des produits à des prix très attractifs afin d'attirer les victimes.

Les risques sont nombreux : produit jamais livré, contrefaçon ou vol des coordonnées bancaires.

Avant tout achat, il est conseillé de vérifier les avis, de privilégier les sites connus, de contrôler la présence du cadenas de sécurité sur le navigateur et d'éviter les paiements par virement à des inconnus.

✓ Les arnaques sentimentales :

Sur les réseaux sociaux ou les sites de rencontre, certains escrocs créent une relation de confiance avant de demander de l'argent sous différents prétextes : urgence médicale, problème familial, voyage ou investissement.

Ces arnaques reposent souvent sur la manipulation émotionnelle. Les fraudeurs jouent souvent sur l'émotion et la compassion.

2/ L'USURPATION D'IDENTITÉ: UNE RISQUE SOUVENT SOUS ESTIMÉ :

L'usurpation d'identité consiste à utiliser les informations personnelles d'une autre personne sans son autorisation.

Les fraudeurs peuvent utiliser une copie de pièce d'identité, un justificatif de domicile, des coordonnées bancaires ou des identifiants numériques afin de réaliser des démarches frauduleuses.

Les conséquences peuvent être importantes : ouverture de comptes bancaires, souscription de crédits, achats au nom de la victime ou difficultés administratives.

3/ QUE FAIRE SI VOUS ÊTES VICTIME D'UNE ARNAQUE :

Lorsqu'une personne est victime d'une fraude ou d'une tentative d'escroquerie, il est important de réagir rapidement afin de limiter les conséquences financières et administratives.



Les personnes âgées sont-elles les seules victimes ?

Non. Les jeunes adultes, les familles, les professionnels et les retraités peuvent tous être ciblés.

Certaines arnaques visent particulièrement :

- ✓ les utilisateurs de réseaux sociaux ;
- ✓ les acheteurs en ligne ;
- ✓ les personnes recherchant un emploi ;
- ✓ les propriétaires ou locataires.



Comment protéger ses mots de passe efficacement ?

Un bon mot de passe doit être :

- ✓ long ;
- ✓ difficile à deviner ;
- ✓ différent pour chaque compte.

Évitez les dates de naissance, prénoms ou suites simples comme « 123456 ».



Prenez quelques minutes pour vérifier.

Un simple contrôle peut éviter des conséquences financières et administratives importantes.

Dans un premier temps, il est conseillé de contacter immédiatement sa banque si des informations bancaires ont été communiquées ou si une opération suspecte apparaît sur le compte. Une opposition sur la carte bancaire peut également être nécessaire.

Il est aussi important de conserver tous les éléments liés à l'arnaque : SMS, e-mails, captures d'écran, relevés bancaires ou échanges avec le fraudeur. Ces documents peuvent être utiles pour effectuer des démarches auprès de la banque, des assurances ou des services de police.

En cas de préjudice, le dépôt de plainte reste recommandé.

✓ En cas d'arnaque en ligne ou de piratage:

Si vous avez cliqué sur un lien frauduleux ou transmis des informations personnelles sur internet, plusieurs réflexes doivent être adoptés rapidement.

Il est conseillé de modifier immédiatement les mots de passe des comptes concernés et d'activer la double authentification lorsque cela est possible. Il est également important de vérifier les connexions récentes à ses comptes et de surveiller toute activité inhabituelle.

Si des coordonnées bancaires ont été communiquées, la banque doit être prévenue sans attendre. Un scan antivirus de l'appareil utilisé peut également permettre de détecter un logiciel malveillant.

Les victimes d'escroqueries sur internet peuvent aussi effectuer un signalement ou déposer plainte en ligne grâce à [la plateforme officielle THESEE](#) (Traitement Harmonisé des Enquêtes et Signalements pour les E-escroqueries).

Cette plateforme permet notamment de signaler :

- les fraudes bancaires ;
- les piratages de comptes ;
- les achats frauduleux en ligne ;
- les arnaques sur internet ou les réseaux sociaux.

✓ En cas d'usurpation d'identité:

Lorsqu'une identité a été utilisée frauduleusement, il est important de déposer plainte rapidement et de conserver toutes les preuves disponibles.

La victime doit également prévenir sa banque ainsi que les organismes concernés afin de limiter les utilisations frauduleuses de ses informations personnelles.

Une surveillance régulière des comptes bancaires et des démarches administratives est recommandée. Dans certaines situations, il peut être nécessaire de renouveler certains documents officiels.

**N'hésitez pas à joindre nos assistantes sociales au 09 80 80 03 07
du lundi au vendredi (hors jours fériés), de 9h à 19h.**