SENIORS

GUIDE DES **ARNAQUES**

Faits
Conseils
Idées

Pays de Normandie
Communauté de Communes

Communauté amie des aînés
CADA

Être senior rime souvent avec le fait d'avoir eu une vie dense et riche d'expérience. La sagesse et la bienveillance qui caractérisent traditionnellement les seniors ne doivent pas faire occulter qu'ils constituent un public ayant des vulnérabilités. Celles-ci sont d'ailleurs exploitées par des individus peu scrupuleux voire malveillants. Il est donc essentiel que les seniors puissent réduire leur exposition à ces menaces.

À cet effet, la gendarmerie du Nord met en oeuvre un ensemble de dispositifs pour assurer la sécurité des aînés. Ainsi et parallèlement à nos actions opérationnelles, la gendarmerie propose la mise en oeuvre de dispositif particulier telle que l'Opération Tranquillité Senior (OTS) qui se traduit par des prises en contact individuel des militaires de la gendarmerie vers les seniors et notamment les plus isolés voire les plus esseulés. Il existe aussi des dispositifs collectifs telle que la Participation Citoyenne qui associe la population à la tranquillité et à la sécurité auxquelles nous aspirons tous. En effet, si les questions d'insécurité relèvent de la gendarmerie, la sécurité est l'affaire de tous.

Par delà ce qui peut être fait par la gendarmerie et les collectivités territoriales pour la sécurité des seniors, il ne doit pas être occulté le fait que les aînés sont aussi en mesure de réduire leur propre vulnérabilité. Ainsi des seniors bien informés seront naturellement moins exposés au risque d'être dupés, abusés et volés. Le guide qui vous est proposé constitue un parfait outil pour réduire cette exposition à des personnes malveillantes.

La gendarmerie du Nord a parfaitement pris en compte le fait que la production de sécurité au profit de la population doit aussi associer cette même population. Concernant plus particulièrement les aînés, la gendarmerie a décidé de lancer une opération de prévention à leur adresse qui a comme singularité de les placer comme acteur du message de prévention et non plus uniquement comme simple récepteur. Le concept de ce dispositif original peut se résumer ainsi : la prévention par et pour les seniors.

Baptisé «Chouettes & Hiboux», cet outil de prévention se traduit par des vidéos présentant certaines situations de vulnérabilité telles que les arnaques aux sentiments sur internet ou encore les vols par ruse aux préjudices des personnes âgées mais aussi par la diffusion de bulletins donnant des conseils sous forme d'infographie parfaitement lisible.

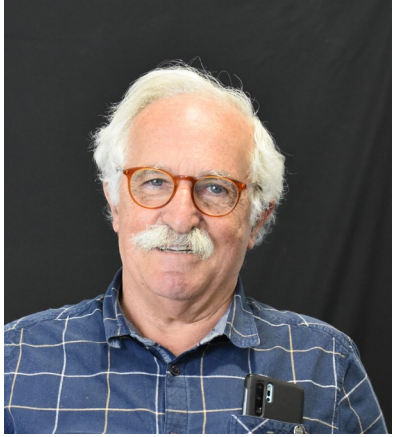
Bien évidemment, la gendarmerie du Nord sera ravie de pouvoir associer les clubs, associations et conseils des aînés de la Communauté de communes du Pays de Mormal au sein du dispositif «Chouettes & Hiboux : la prévention par & pour les seniors».

Lieutenant - Colonel Laurent GLADIEUX
commandant en second la Gendarmerie du Nord

Dispositif «Chouettes & Hiboux : la prévention par & pour les seniors»

Harcèlement, violences, escroqueries, vols, agressions et dangers d'internet
Prévention rapide simple et efficace, des bons conseils, des bonnes adresses, des infos pratiques

GENDARMERIE
NOTRE ENGAGEMENT, VOTRE SÉCURITÉ



Christian Dorlodot

Référent élu du groupe Communication de la Communauté Amie des Aînés

Ce recueil des arnaques connues a été réalisé par le groupe de travail communication de la Communauté amie des aînés constitué de seniors et de techniciens de la communauté de communes du Pays de Mormal dont je suis le référent élu.
Il a été imaginé pour prévenir un public de personnes âgées, mais lors de nos recherches et de l'écriture du texte nous nous sommes vite rendu compte qu'il devrait intéresser aussi tout un chacun et de tout âge.
Nous avons essayé de traiter une majorité des arnaques actuelles que nous avons recensées, toutefois les arnaqueurs, de plus en plus nombreux, cherchent continuellement à inventer de nouveaux stratagèmes. Donc méfiance !!!!
De plus la génération des personnes âgées a vécu une époque où le respect de l'autre était courant. La méfiance vis-à-vis des personnes rencontrées était moins grande. Aujourd'hui ce respect des autres et du bien d'autrui n'existe plus forcément toujours. Il faut désormais que nos aînés apprennent à reconnaitre les arnaqueurs et autres escrocs qui peuvent les entourer.
Nous avons eu le plaisir et l'extrême honneur d'être aidés dans nos travaux d'écriture par les services de la gendarmerie nationale qui ont bien voulu vérifier les textes, partager leurs connaissances et au final valider le guide. Nous les remercions sincèrement et chaleureusement pour ce partenariat inédit.
La gendarmerie nationale, en préfaçant ce recueil, rappelle que les gendarmes oeuvrant sur le territoire sont à votre service, n'hésitez pas à faire appel à eux, vous les aiderez dans l'accomplissement de leurs tâches et la résolution d'affaires bien plus que vous ne le pensez.
Nous souhaitons que ce recueil vous apporte des informations, des astuces, vis-à-vis de ce monde de plus en plus dématérialisé qui nous entoure. Il sera plus difficile alors pour les piégeurs de vous faire tomber dans le panneau par crédulité.

Bonne lecture à tous !

Sommaire

1

À **DOMICILE**

Démarchages et demandes téléphoniques

Les escroqueries téléphoniques sont un problème qui prend de l'ampleur. Les signalements au numéro d'alerte des opérateurs (n° 33700) ont augmenté sensiblement.

Ces escroqueries sont de différents ordres :

1. Le spam vocal
2. La fraude aux besoins urgents, aux demandes de paiement
3. Les manipulations
4. Les demandes de renseignements confidentiels
5. Les arnaques techniques
6. L'arnaque « sanitaire »
7. L'arnaque sur l'isolation à 1€

1) Le spam vocal

Les arnaqueurs incitent la victime à rappeler un numéro surtaxé. Celui-ci ne commence pas toujours par 08. Il peut être un numéro à 4 chiffres qui commence par 3. Les fraudeurs utilisent un numéro classique 01, 02,...

En voici quelques exemples :

- Le téléphone sonne une fois. Vous n'avez pas le temps de décrocher.
- « Allô, allô, ah mince je n'entends pas, rappelle-moi ». La communication est coupée. Il s'agit d'un enregistrement sonore. Si vous appuyez sur le bouton « rappeler » vous obtenez un numéro surtaxé.
- Les messages pré-enregistrés. Vous entendez « il y a un problème de facturation. Appelez en urgence ». En se faisant passer pour votre banque ou le centre des impôts, vous êtes invité à rappeler d'urgence un serveur surtaxé.
  Ces deux méthodes créent un effet de stress chez le destinataire qui pense devoir régler la situation en urgence.

Dans le même ordre d'idée que le spam vocal, les SMS ou textos peuvent vous amener à utiliser un numéro surtaxé.

- Par SMS : « Vous avez un colis en attente, merci de confirmer l'heure de livraison ».
- Se méfier des messages : « vous avez gagné... », « vos identifiants ont été volés » !

2) La fraude aux besoins urgents, aux demandes de paiement

Comme sur internet, il existe aussi des fraudes aux demandes d'aides, aux dépannages en urgence :
« J'ai perdu mon téléphone (on me l'a volé) ... » « On m'a dérobé mon portefeuille je n'ai plus d'agent pour rentrer ».

Un notaire vous apprend que vous êtes bénéficiaire d'un contrat d'assurance vie. Par téléphone, ou par mail, une personne s'appuyant sur l'usurpation d'identité d'un notaire cible les proches d'une personne décédée grâce aux avis d'obsèques. Après avoir envoyé les pièces demandées (identité, livret de famille ...) un faux certificat notarial leur parvient avec une demande de paiement pour débloquer les fonds.

Il faut vérifier que vous êtes bien bénéficiaire d'un contrat d'assurance vie en adressant une demande à l'AGIRA (Association pour la Gestion des Informations sur le Risque en Assurance) accompagnée d'un acte de décès et des noms et adresse des bénéficiaires. L'AGIRA transmettra la demande à tous les assureurs qui vous contacteront si vous êtes bénéficiaires.

Attention ! **Un notaire peut avoir connaissance de l'existence d'un contrat d'assurance vie, mais ne peut pas être en possession des fonds placés qui restent entre les mains des assureurs qui sont les seuls à pouvoir les débloquer.**

3) La manipulation

Moins connu, le manipulateur de marchés. Vous recevez un appel ou un SMS vous proposant un placement dans certaines actions. Le promoteur en détient aussi ; au fur et à mesure qu'il « recrute » de nouveaux acheteurs, le cours monte. Lorsqu'il atteint un certain niveau le fraudeur vend, le cours s'effondre et vos actions n'ont plus de valeur boursière.

4) Les demandes de renseignements confidentiels

La gendarmerie ou la police vous appelle : « nous avons arrêté deux individus en possession de vos coordonnées bancaires » puis vous pose des questions sur la façon de faire vos achats, si vous réglez par carte. Ensuite elle vous demande vos coordonnées bancaires sous prétexte de vérification.

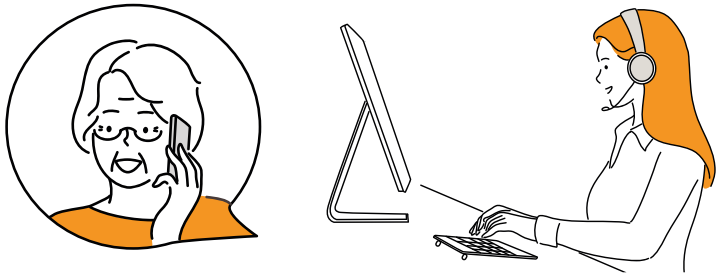
5) LES ARNAQUES techniques

Appel du service technique d'un opérateur pour nettoyer le téléphone atteint d'un virus. Il est demandé de rappeler un numéro situé à l'étranger et surtaxé. Votre appel peut durer un certain temps.

Une dame se présentant comme salariée d'un opérateur téléphonique appelle une « mamie » de 88 ans. Elle semble tout savoir de ses abonnements Télécom et parle un Français parfait. La requête formulée était plausible : la « technicienne » lui a indiqué devoir procéder à des vérifications sur la ligne et a demandé à « mamie » de la rappeler. Après avoir passé 40 minutes à attendre, elle a raccroché.

La « technicienne » la rappelle et lui demande de rester en ligne en lui assurant que tout était gratuit et lui fait peur en lui disant que sa ligne téléphonique et son abonnement télé risquaient d'être coupés. Au final, 6 appels passés, coût hors forfait de 355 euros pour des appels passés en Afrique.

« Mamie » a été victime d'une nouvelle forme d'arnaque. L'unique but est de rester longtemps en ligne. Le numéro à rappeler commence généralement par 00. La facture est toujours salée. Le recours vain, les opérateurs n'acceptant des dédommagements qu'aux cas par cas.



Les renseignements téléphoniques, le remplacement du 12 par des numéros 118... est un fiasco. Les tarifs n'ont cessé d'augmenter. Certains 118 profitent de votre appel pour vous proposer des services (réservation de billets par exemple).

6) LES ARNAQUES sanitaires

L'arnaque aux faux kits. Recevoir des masques, du gel, des gants pour un faible coût. Rappeler un n° surtaxé pour les obtenir.
Egalement pour obtenir un rendez-vous dans un centre de vaccinations.

Les démarcheurs abusifs ciblent surtout les personnes âgées, plus susceptibles de se laisser convaincre, en se basant sur les prénoms dans l'annuaire ou sur les boîtes aux lettres. De manière générale, n'hésitez pas à mettre votre entourage au courant du risque d'arnaque à l'isolation pour 1 euro.

7) LES ARNAQUES sur l'isolation à 1 euro

1. Constat

Depuis quelques mois, difficile de passer à côté des reportages et témoignages sur les arnaques d'isolation à 1 euro (Envoyé Spécial sur France 2, Grands Reportages sur TF1, etc.). **Malgré l'existence** avérée de ce dispositif de financement, pour isoler les combles par exemple, on constate divers abus et comportements malveillants de la part d'entreprises peu scrupuleuses, voire de véritables escrocs professionnels.
Chaque année plus d'un million de ménages engagent des travaux de rénovation énergétique.
En effet, suite à la plainte de nombreux propriétaires abusés, la DGCCRF réalise des enquêtes et des contrôles auprès des entreprises et artisans réalisant des travaux de rénovation énergétique.

Ainsi, ces travaux révèlent de nombreuses fraudes telles que :

- la présentation de devis incompréhensibles pour les consommateurs
- des crédits camouflés
- des labels de qualité mensongers
- des pratiques commerciales trompeuses
- le non-respect des droits du consommateur
- des manquements relatifs à l'information sur les prix.
- Des travaux mal faits : par exemple isolant mal posé, mauvais matériau utilisé (très dangereux si inflammable), espaces laissés entre les rouleaux, etc.
- L'avance des frais : certaines personnes finissent par souscrire des prêts à la consommation de plusieurs milliers d'euros.

Attention ! **Le démarchage téléphonique concernant les travaux de rénovation énergétique est interdit depuis le 25 juillet 2020. Dans le cas d'un démarchage, il ne faut jamais signer d'engagement. Prendre le temps de réfléchir et ne pas verser d'acompte le jour même. Vérifier les informations qui ont été transmises, comme l'identité du professionnel et les données chiffrées avancées.**

2. Rénovation énergétique : Nos conseils pour bien choisir les professionnels

Afin de vous prémunir contre les risques éventuels de faire appel à un professionnel douteux, voici quelques réflexes à avoir pour réaliser les travaux énergétiques de votre logement en toute sérénité.

2.1. Ne signez pas d'engagement lorsqu'une entreprise vient vous démarcher.

- Laissez-vous le temps de la réflexion et de la compréhension. Vérifiez les informations qui vous ont été transmises, en particulier **l'identité du professionnel** et **les données chiffrée**s avancées.

- Méfiez-vous tout particulièrement des entreprises prétendant être mandatées par un organisme public, car **les services publics ne démarchent jamais**, que ça soit par internet, par téléphone ou au domicile.

- Avant de signer, lisez bien l'intégralité du ou des documents. Si vous avez signé et regrettez, n'hésitez pas à faire valoir votre **droit à la rétractation** prévu par la loi dans un délai de 14 jours.

2.2. Avant de vous lancer dans des travaux faites quelques vérifications

- En cas de doute sur un professionnel ou de question, **contactez un conseiller FAIRE** (Faciliter, Accompagner et Informer pour la Rénovation Énergétique) au 0 808 800 700 ou sur le site internet **faire.fr** le service public qui vous guide dans vos travaux de rénovation énergétique.

- Examinez la qualité des sites Internet ou de la documentation fournie et la lire avec attention préalablement à la signature.

- Comparez les prestations et les prix avec d'autres professionnels. Prenez le temps de comparer les offres en contactant plusieurs entreprises, surtout si vous avez été démarché.

- Contrôlez le label du professionnel : si vous souhaitez bénéficier du crédit d'impôt transition énergétique (CITE) et de l'éco-prêt à taux zéro (éco PTZ), vous devez choisir un professionnel labellisé « garant de l'environnement » (RGE). Pour trouver un professionnel RGE ou vérifier que le professionnel que vous engagez est bien labellisé RGE (consultez l'annuaire des professionnels RGE). Attention cependant, être labellisé RGE ne garantit pas que l'entreprise n'ait pas de pratiques commerciales trompeuses.

2.3. En cas de financement des travaux par un prêt, soyez vigilant

- Prenez connaissance attentivement de l'exemplaire papier de l'offre de crédit qui doit obligatoirement être remis par l'organisme bancaire.

- Soyez vigilant en cas de remboursement différé des premières mensualités. De telles modalités peuvent contribuer à augmenter significativement le coût total du prêt.

- Soyez vigilant à l'attestation de fin de travaux, qui confirme la conformité de la prestation rendue et marque le début des obligations de remboursement.

2.4. En cas de travaux ne s'étant pas déroulés comme prévu, faîtes-vous assister

- Faites une réclamation via le formulaire présent sur le site internet de **faire.fr** pour des travaux réalisés par une entreprise RGE.

- Saisissez le médiateur de la consommation choisi par le professionnel en cas de litige. Ses coordonnées doivent être présentes sur les documents contractuels. La procédure est gratuite.

- Faites-vous assister par une association agréée de protection des consommateurs en cas de besoin.

- Signalez les manquements du professionnel en contactant la direction départementale de la cohésion sociale et de la protection des populations (DDCSPP) du département et assignez le professionnel devant le juge civil pour tout contentieux lié à l'exécution du contrat.

- Consultez votre assurance habitation (protection juridique).

Le 1er juillet 2021, le coup de pouce «isolation des combles et planchers» a été modifié afin de mettre fin aux offres à 1 euro.

Les primes « coup de pouce énergie »
Chauffage, isolation, rénovation globale... Plusieurs primes dites «coup de pouce énergie» vous permettent de financer certains travaux de rénovation énergétique.

Rénovation énergétique : soyez vigilant !

Comment éviter LES ARNAQUES aux démarchages et demandes téléphoniques ? QUE FAIRE si cela arrive ?

• Ne pas afficher son numéro de téléphone, par exemple sur une voiture à vendre.

• Se méfier lorsque l'on demande de fournir des renseignements personnels ou financiers ; de la phrase : « surtout ne raccrochez pas » ...

• Eviter de répondre à des numéros inconnus. Si votre correspondant vous connait, il vous rappellera ou vous laissera un message.

• Inscrivez-vous gratuitement sur les listes rouge ou orange de votre opérateur téléphonique :

liste rouge : les coordonnées ne seront pas mentionnées sur les listes d'abonnés ou d'utilisateurs

liste orange : les coordonnées ne seront plus communiquées à des entreprises commerciales en vue d'une utilisation pour prospection directe.

L'inscription sur ces listes permet seulement de ne pas figurer dans les annuaires. Mais les prospecteurs peuvent se procurer des données en les achetant auprès d'acteurs spécialisés sur le net.

• Vous pouvez toujours raccrocher sans avoir à vous justifier.

• En cas d'appels surtaxés et de refus de remboursement de votre opérateur, vous pouvez faire appel à la médiatrice des télécommunications (sur internet rechercher «médiatrice des intercommunications»).

• Signaler le numéro frauduleux au 33700. Envoi d'un SMS en inscrivant : SPAM VOCAL suivi du NUMERO FRAUDULEUX ou de faire un signalement sur la plateforme **33700.fr**.

Astuce ! **Vous ne souhaitez pas faire apparaitre votre numéro de téléphone portable en appelant votre correspondant : vous inscrivez #31# avant le numéro. La mention « numéro privé » s'affichera sur le téléphone de votre correspondant.**

Dépannage

Quelles sont les précautions à prendre vis-à-vis des entreprises intervenant chez un particulier ?

Les vols lors des interventions d'entreprises chez un particulier sont fréquents et bien plus encore lorsque les propriétaires sont des personnes âgées, en difficulté visuelle, auditive ou de mobilité.

Même si une entreprise ou un artisan a pignon sur rue, le personnel embauché, l'est généralement sur des critères de compétences, mais pas forcément d'honnêteté. Surtout à certaines périodes de l'année où les intérimaires sont légion. Une méfiance particulière doit donc être prodiguée.

Il est difficile, voire impossible, pour des personnes âgées de surveiller les entreprises ou artisans qui interviennent chez eux.

Comment limiter cela ?

Certaines précautions sont à prendre.

Le choix de l'entreprise

Ne jamais prendre une entreprise qui n'a pas pignon sur rue. Elle doit être choisie dans le tissu local et posséder un numéro de Siret.

Consulter des personnes de confiance pour savoir si elles ont déjà fait appel à cette entreprise, si elle répond aux besoins et ce qu'elles en pensent.

Refuser toute proposition d'une personne qui vous offre des services en sonnant à votre porte en vous promettant des interventions rapides sur vos toitures, le ramonage de vos cheminées, de macadamiser votre cour ou toute autre intervention de courte durée.

L'entreprise doit vous remettre un devis précisant la description détaillée des travaux (faire vérifier par un proche compétent le bien-fondé et l'utilité de la totalité du devis), le prix, les dates de début et de fin de travaux et conditions de paiements.

Ce devis signé scelle un accord écrit qui vous engage ainsi que l'entreprise concernée.

Lors des travaux

Faire en sorte qu'une personne soit toujours présente lorsque l'entreprise est sur place.

Essayer de limiter le déplacement des intervenants aux pièces nécessaires, en fermant certaines portes ou accès.

Essayer de surveiller les allées et venues entre les véhicules de la société et le lieu de travaux.

Demander à la société de ne pas se disperser et d'intervenir pièce par pièce.

Ne pas laisser trainer sur les lieux des travaux des objets pouvant être convoités. Ne pas garder à proximité de l'argent, des bijoux et autres objets de valeur, voir vos propres outils.

Ne pas apparaitre devant les ouvriers portant bijoux et objet de valeur.
Ne pas aller chercher quelque chose dans une pièce voisine ou en dehors de la maison à la demande d'un ouvrier.

A la fin des travaux, faire le tour du chantier avec un représentant de l'entreprise exécutrice et bien vérifier que tout est en place et que rien n'a disparu.

En cas de vol constaté après l'intervention ne pas hésiter à porter plainte auprès de la gendarmerie.

Intrusion

Les vols et cambriolages sont particulièrement constatés au sein des domiciles de personnes âgées. Elles gardent chez elle des grosses sommes d'argent liquide et/ou des bijoux de famille, ce qui est une aubaine pour les voleurs.

Le vol par ruse ou vol avec ruse est aussi appelé vol à la fausse identité. Les voleurs procèdent par usurpation d'identité afin d'obtenir l'accès à l'habitation.

Le stratagème du vol est simple : un des voleurs sonne chez la victime en se faisant passer pour un agent de la compagnie d'eau, ou encore un policier, un gendarme ou un pompier. Une fois rentré au domicile, il détourne alors l'attention de la victime en la dirigeant vers la cuisine, la salle de bains ou encore le garage. Pendant ce temps, un complice s'introduit dans le domicile et dérobe alors tout ce qui lui tombe sous la main.

Ces vols ont souvent lieu en semaine, pendant la journée, prenant pour cible les personnes de 70 ans ou plus et vivant seules.

D'autres modes de malversations, escroqueries, abus de faiblesse, détournement d'argent, cambriolages existent. Les voleurs et larrons en tous genres ne manquent pas d'imagination !

En voici quelques exemples :

A Dunkerque : un assureur avait amassé plusieurs centaines de milliers d'euros pendant 14 ans en les récupérant auprès de personnes âgées vulnérables.

En Bretagne, une dame de 84 ans hospitalisée ainsi que son compagnon en grand état de faiblesse ont été abusés par sa fille et son compagnon : en trois mois 23 chèques ou retraits d'argent par carte bancaire ont été effectués à leurs dépens.

Un monsieur âgé de 85 ans qui habite dans une petite maison vétuste se fait vendre, par un démarcheur à domicile peu scrupuleux, une pompe à chaleur d'une valeur de plus du double des prix généralement pratiqués et installée… dans son grenier !

Le fait de voler une personne âgée en abusant de sa confiance, en profitant de son âge et de sa faiblesse physique est ressenti comme une agression, même s'il n'y a pas de séquelles physiques, et plonge fréquemment la victime dans une détresse morale et psychologique. Il s'agit d'un abus de faiblesse.

Quelques astuces suffisent parfois pour se prémunir d'un vol par ruse

→ Utiliser un judas de porte ou un entrebâilleur

Lorsqu'on sonne ou frappe à la porte, le premier réflexe est de regarder à qui vous avez affaire. Si vous disposez d'un visiophone, vous pouvez observer dans un premier temps votre interlocuteur et vous entretenir avec lui avant de le laisser entrer ou non chez vous. Même chose si vous disposez d'un judas de porte, aussi appelé « œil-de-bœuf », ou d'un entrebâilleur. Ne laissez entrer personne si vous avez un soupçon.

→ Vérifier l'identité de la personne

Deuxième étape pour éviter d'être victime d'un vol par ruse, vérifiez l'identité de la personne avant de la laisser pénétrer chez vous. Exigez la présentation de sa carte professionnelle, même si la personne face à vous est en tenue d'uniforme. Rien ne prouve qu'il ne s'agit pas d'un faux uniforme. Mais il peut aussi s'agir d'une fausse carte. Vous pouvez donc aussi vérifier l'identité de la personne en contactant la société censée embaucher cet individu. Si l'individu vous donne lui-même un numéro, il peut s'agir d'un complice au téléphone. Cherchez le numéro de la société par vous-même, et une fois votre interlocuteur en ligne, vérifiez que le nom, le prénom et le lieu de l'intervention correspondent bien.

→ Verrouiller la porte derrière soi

Si vous laissez entrer le visiteur, fermez la porte d'entrée à clé une fois qu'il est rentré. En effet, dans le cas d'une tentative de vol par ruse, le malfaiteur tentera de laisser la porte entrouverte derrière lui pour permettre à un complice de s'introduire dans votre logement pour vous dérober vos biens. Verrouillez donc la porte et restez avec le visiteur afin de ne pas le laisser seul chez vous.

→ Ne laissez entrer personne si vous ne le voulez pas

Pour éviter un cambriolage, si vous avez un soupçon, un doute, ne laissez entrer personne chez vous, même un policier. **Vous êtes chez vous, c'est donc vous et vous seul qui décidez**. Sauf mandat d'arrêt ou de perquisition, personne ne peut entrer à votre domicile sans votre accord. Si le visiteur insiste, appelez les forces de l'ordre.

→ Méfiez-vous des personnes que vous ne connaissez pas qui vous demandent de les aider à chercher un chien ou un chat entré dans votre jardin ou dans votre propriété. Si vous acceptez de les aider, fermez à clé votre maison avant de sortir. En effet un complice peut entrer chez vous pendant que vous cherchez l'animal dans votre jardin. Une fois le forfait réalisé, le « propriétaire » du chien ou du chat abandonnera les recherches.

Les vols en votre absence, comment les éviter ?

- **N'inscrivez pas de mention sur la boite aux lettres permettant de savoir que vous êtes seul-e. N'indiquez que le nom de famille.**
- **Ne suspendez pas les clés près de la porte, ne les mettez pas sous le paillasson ou dans un pot de fleurs près de la porte.**
- **En cas d'absence prolongée, avisez vos voisins de votre départ si vous êtes sûr d'eux**
- **Faites ouvrir régulièrement les volets, vider la boite aux lettres et sortir les bacs de déchets pour faire paraitre votre résidence habitée.**
- **Ne laissez pas de message indiquant votre absence (répondeurs, réseaux sociaux).**
- **Placez vos objets de valeur en lieu sûr : les piles de linge sont les cachettes les plus connues !**
- **Mettez vos documents de valeur importants sous clé (bureau, secrétaire, caisse métallique).**
- **Signalez votre absence à la gendarmerie dans le cadre de l'opération tranquillité vacances.**

ARNAQUES **FINANCIÈRES**

Règlements bancaires

LES FRAUDES BANCAIRES EN FRANCE, quelques chiffres

En 2018, le montant de la fraude bancaire en France a atteint environ 538 millions d'euros. Les escroqueries et infractions économiques et financières ont fortement augmenté ces dernières années avec le développement des nouveaux moyens de paiement et l'utilisation frauduleuse des informations bancaires, grâce au détournement des réseaux de communication où circulent ces données.

57 300
Nombre de falsifications et d'usages de cartes de crédit en France

27 200
Nombre de falsifications et d'usages de chèques volés en France

900
Nombre d'infractions relatives aux faux-monneyage en France

Paul Manuel Godoy Hilario, 12 nov. 2020

LES DIFFERENTS MODES DE FRAUDE A LA CARTE BANCAIRE

1. Le phishing ou l'hameçonnage ou encore filoutage

L'hameçonnage ou phishing en anglais est une technique très répandue que vous devez savoir reconnaitre.

Le phishing est une forme de **cybercriminalité** dans laquelle la victime (potentielle) est approchée par de faux e-mail, sms, messagerie instantanée, médias sociaux ou téléphone. L'escroc se fait passer pour quelqu'un d'autre. Il peut s'agir de votre banque, fournisseur d'énergie ou d'une société de technologie, mais aussi d'un ami ou d'un membre de la famille.

Le but est de «pêcher» («phishing» en anglais) des données sensibles, comme des informations personnelles, des mots de passe, des données de carte bancaire ou de crédit. Une fois qu'il s'est emparé de ces données, l'escroc a les coudées franches : il peut par exemple accéder aux principaux comptes de la victime et ainsi dérober son argent ou usurper son identité.

Une usurpation d'identité est une **utilisation de données personnelles propres à vous identifier sans votre accord.** Une fois volées, ces informations peuvent servir aux usurpateurs pour nuire à votre réputation, réaliser des opérations financières ou commettre des actes répréhensibles en votre nom.

Les usurpateurs peuvent voler vos données via un piratage ou se faire passer pour un organisme privé ou public connu, dans le but d'instaurer un climat de confiance et de vous amener à donner des informations personnelles. Les cybercriminels tentent de vous duper, de vous angoisser. Ne vous laissez pas attraper, l'adresse mail doit vous alerter.

➜ Exemple de mail bancaire frauduleux :

Le courriel reçu par Monsieur C. semblait provenir de sa banque, le LCL.

De : LCL@notif.lcl.fr <servicegroupelng6991402@purequest.com>
Envoyé : mardi 24 septembre 2019 13:01
À :
Objet :

Cher(e) client(e),
Nous vous invitons à consulter votre compte pour mettre à jour votre Numéro de téléphone.
Rendez-vous dans votre Espace Client , Lors du processus de la mise à jour, vous êtes amené à définir un code à 6 chiffres.
Nous restons à votre disposition pour tout renseignement lié à l'utilisation des services de gestion de comptes.

A bientôt sur nos sites.

Attention, il est inutile de répondre à ce message, votre mail ne fera l'objet d'aucun traitement.

Bien cordialement,
LCL

Ne pas répondre à cet accusé de réception: il ne sera pas traité.

IMPORTANT : LCL ne vous sollicite jamais (que ce soit par mail, par SMS ou par téléphone) pour vous demander de communiquer de quelque manière que ce soit votre code personnel d'accès à ses services. Si vous recevez un tel message, ne cliquez sur aucun lien, n'appelez pas le numéro indiqué et ne tenez pas compte des informations qu'il contient. Il s'agit sans doute d'un message de phishing à faire simplement suivre à l'adresse alerte@securite.lcl.fr

Jérémie HENEMAN
Service Clientèle en Ligne

2. La fraude à la carte bancaire

Il y a plusieurs possibilités :

- Copie de la bande magnétique par un commerçant
- Site frauduleux
- Caméra
- Faux lecteur de carte ou encore faux clavier placés sur un distributeur de billets...

Les possibilités sont quasiment infinies.

Astuce Mettez votre carte bancaire dans une pochette antipiratage

3. La fraude au prélèvement SEPA

Le système SEPA harmonise les moyens de paiement et fluidifie les transferts de fonds entre les pays d'Europe. Seul hic, faire un prélèvement est désormais si facile que certains individus peu scrupuleux profitent de la situation pour opérer des prélèvements non-autorisés.

Comment ça marche ?

Toute personne en possession de votre RIB, et donc de vos coordonnées bancaires, peut mettre en place un prélèvement sur votre compte en banque. Il n'est en effet pas obligatoire pour une banque de vérifier que la demande de prélèvement s'appuie bien sur une autorisation préalable de votre part. C'est à vous d'être vigilant et de contrôler vos comptes afin d'obtenir le cas échéant le remboursement.

Certains fraudeurs peuvent également utiliser vos informations bancaires pour falsifier un mandat de prélèvement TIP (Titre interbancaire de paiement) et effectuer un prélèvement faussement autorisé sur votre compte.

4. Les fraudes et arnaques au chèque

Payer par chèque

Lorsque vous émettez un chèque, celui-ci peut être falsifié de deux manières :

-> Soit la somme indiquée est modifiée,
-> Soit c'est le nom du bénéficiaire qui fait l'objet d'un changement.

Si le destinataire de votre chèque vous signale qu'il n'a pas reçu votre paiement alors que vous êtes débité : faites opposition auprès de votre banque et portez plainte pour fraude.

Votre banque doit vous rembourser le montant extorqué si le chèque a été modifié de façon visible.

En revanche si la falsification est difficilement décelable, votre banque n'est pas tenue de vous reverser les fonds.

Quelques précautions :

- Remplissez toujours toutes les informations demandées,
- Ne laissez pas d'espaces vides,
- Utilisez un stylo à bille noire classique

Astuce ! **Lors de l'envoi d'un chèque, mettez un morceau de ruban adhésif transparent et mat sur la somme, le nom du récipiendaire et les chiffres.**

Recevoir un chèque en paiement

Prenez garde, le chèque n'est pas le moyen de paiement le plus fiable : un chèque peut tout à fait se révéler sans provision ou invalide.

Afin d'éviter de voir votre chèque refusé par votre banque certaines précautions s'imposent :

• Vérifiez que toutes les informations demandées sur le chèque sont bien complétées,

• Assurez-vous que le montant indiqué en chiffres correspond à celui indiqué en lettres,

• Contrôlez la justesse de la date indiquée (attention un chèque ne peut plus être encaissé après 1 an et 8 jours),

• Vérifiez que le nom et l'adresse apparaissent bien sur le chèque et que les coordonnées de la banque y figurent également.

L'arnaque au chèque

Un supposé client vous fait une demande de devis, accepte l'offre proposée et verse très rapidement un acompte ou procède au règlement anticipé de la prestation.

Mais le montant versé est supérieur à celui indiqué sur le devis, 2 000 euros au lieu de 200 euros par exemple. Le faux client allègue une erreur et vous demande la restitution de la somme excédentaire.

Constatant que les fonds apparaissent bien votre compte, vous vous empressez de faire un virement afin de le rembourser. Le piège se referme lorsque votre banque vous signale que les sommes envoyées initialement par le supposé client n'ont finalement pas été créditées sur votre compte.

L'explication ?

Lorsque vous déposez un chèque, la somme correspondante apparait sur votre compte au bout d'un jour ouvré (pour les chèques en euros).

Mais attention, cet argent n'est pas réellement disponible ! Un délai variable de 8 jours à environ 1 mois est nécessaire pour que le chèque soit vérifié par votre banque et crédité à titre définitif. En cas de chèque en bois, les sommes disparaissent donc de votre compte.

Autre précision importante :
La même arnaque peut être réalisée par l'utilisation de votre RIB.

Comment éviter LES FRAUDES BANCAIRES ?

Rassurez-vous cependant : certains indices mettent la puce à l'oreille et permettent de se protéger. Pour que le Web reste un havre de paix, suivez nos conseils.

→ 1. Je consulte régulièrement les consignes de sécurité de ma banque

Les banques publient régulièrement sur leur site, dans une rubrique consacrée à la sécurité, des conseils et alertes.

Consultez-la régulièrement et appliquez les consignes.

→ 2. Je choisis avec soin mon mot de passe

Le service cyber malveillance du gouvernement recommande de choisir un mot de passe différent pour chaque compte.

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-choisir-un-bon-mot-de-passe

Le mot de passe doit être complexe, afin que personne ne puisse le deviner, pas même votre famille ou votre entourage. Il doit comporter au minimum 8 à 12 caractères mélangeant les majuscules, les minuscules, des chiffres et des caractères spéciaux.

Lorsque vous choisissez votre mot de passe, évitez donc toutes les informations qui vous concernent et qui sont facilement accessibles (sur vos réseaux sociaux par exemple) :

- Dates de naissance de vos proches
- Noms de vos proches
- Noms de vos animaux de compagnie
- Etc.

2 méthodes pour créer un mot de passe sécurisé

Créer soi-même son mot de passe

Le mot de passe doit être long et complexe avec des lettres (majuscules et minuscules), des chiffres, de la ponctuation, des caractères spéciaux et n'avoir aucun rapport avec votre vie personnelle.

Conseils pour vous en souvenir :

› Retenir la ou les premières lettres de chaque mot composant une phrase

› Utiliser la phonétique d'une phrase pour créer une suite de lettres et de chiffres correspondant

› Créer une méthode connue de vous seul

Utiliser un générateur de mots de passe

Il est possible d'utiliser un générateur de mots de passe qui se chargera de les inventer pour vous.

Le gestionnaire de mots de passe KeePass, logiciel gratuit et certifié par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), propose une fonctionnalité de génération de mots de passe complexes et aléatoires.

Ils seront alors plus compliqués à mémoriser que ceux que vous créez. KeePass dispose aussi d'une fonction qui permet de stocker vos mots de passe en toute sécurité.

→ 3. Je garde secrets mes codes d'accès

Ne communiquez jamais votre mot de passe à une personne de votre entourage, quelle qu'elle soit. L'idée n'est pas d'être méfiant à outrance mais de rester vigilant : les enjeux sont tels que votre mot de passe doit rester totalement confidentiel.

Jamais aucune entreprise ou service d'État ne vous le demandera par téléphone ou par courriel. Si vous recevez une telle sollicitation, c'est qu'il s'agit d'une tentative d'arnaque par hameçonnage.

→ 4. Je ne me connecte jamais à partir d'un courrier électronique ou SMS

(a.) En cas de tentative de phishing

Ne jamais utiliser le lien figurant dans un courrier électronique pour vous connecter à votre site de banque à distance, quel qu'en soit l'objet.

Passer par l'adresse du site internet de votre banque…

Ne jamais répondre à un courrier électronique douteux et utilisant les coordonnées ou l'identité (logo, visuel…) de votre banque surtout si l'objet est alarmiste et demande une action urgente.

Ne jamais fournir d'informations à l'expéditeur d'un tel message. Prévenir votre banque au plus vite en lui faisant suivre le message.

(b.) En cas de tentative de Smishing

Ne pas répondre à un SMS vous demandant d'appeler un numéro, de vous connecter à un site depuis votre téléphone.

Transmettre le SMS au 33700 mis en place par les principaux opérateurs français : plus d'informations sur

www.33700-spam-sms.fr

Le pishing kézako ?

Le pishing est une technique consistant à récupérer les informations confidentielles des internautes via différents biais : faux e-mails, piratage de sites web … Ce procédé est très utilisé par les pirates informatiques modernes.

Le smishing kézako ?

Le smishing est une forme de phishing dans laquelle un attaquant utilise un SMS convaincant pour inciter les destinataires ciblés à cliquer sur un lien et à envoyer à l'attaquant des informations privées ou à télécharger des programmes malveillants sur un smartphone.

→ 5. Je contacte ma banque en cas de doute

Si vous pensez avoir fourni vos codes d'accès de banque à distance à un tiers via un site internet, un lien SMS ou directement par téléphone, contactez immédiatement votre banque, aux coordonnées habituelles, pour lui signaler (n'utilisez pas celles des messages que vous venez de recevoir).

Sans attendre les instructions de la banque, lancez l'antivirus, changez vos codes d'accès, vérifiez les dernières opérations effectuées.

→ 6. Je consulte régulièrement mon compte

Vérifiez le contenu de votre relevé de compte dès sa réception notamment avec les talons des chèques émis, les facturettes de carte et les courriels de confirmation de paiement (fournis la plupart du temps pour les achats par internet).

Connectez-vous au moins une fois par semaine sur le site de votre banque à distance ou votre application mobile.

→ 7. Je signale rapidement toute anomalie

En cas de doute sur une opération, demandez sans attendre des précisions à votre banque.

→ 8. Je réagis en cas d'activité suspecte sur mon téléphone

Si vous recevez un SMS de sécurité alors que vous n'êtes pas en train de faire une opération « sensible » ou un achat en ligne, il s'agit sans doute d'une tentative de fraude ou d'une erreur de coordonnées téléphoniques.

Une ligne téléphonique peut être détournée et être utilisée pour effectuer des tentatives de fraudes bancaires sur vos comptes.

→ 9. Je protège mon matériel

La sécurisation de vos terminaux (ordinateur, téléphone portable, tablette, etc.) est primordiale. Vous devez lutter contre les virus et logiciels malveillants (malwares) de tous types.

Il peut s'agir de :

> **Spyware :** logiciel espion qui collecte les données personnelles et les envoie à un tiers

> **Keylogger :** logiciel spécialisé pour espionner les frappes au clavier, il peut recueillir les mots de passe, les codes de carte bancaires, etc.

> **Backdoor :** logiciel qui permet au pirate de prendre le contrôle de l'ordinateur…

Téléchargez régulièrement les mises à jour système, installez sur votre ordinateur comme sur votre mobile un antivirus et un pare-feu efficaces avec des mises à jour automatiques.

N'ouvrez pas un message douteux (objet et contenu passe-partout), surtout si une pièce jointe est attachée, détruisez-le sans l'ouvrir.

N'effectuez aucune opération de banque à distance (connexion, virement, opposition …) si vous pensez avoir un virus sur votre ordinateur, lancez l'antivirus pour nettoyer l'ordinateur puis contactez votre agence pour demander de nouveaux codes d'accès.

N'utilisez pas l'équipement dont vous ne maitrisez pas le niveau de sécurité (cybercafé, libre-service …).

Ne téléchargez que les programmes et contenus (photos, vidéos, sonneries, thèmes pour mobile et jeux) provenant d'une source fiable.

→ 10. Je sécurise mes connexions

Choisissez un fournisseur d'accès internet reconnu et suivez ses conseils de sécurité.

Vérifier la présence de https (« s » pour secure) devant l'adresse du site, icône d'une clé ou d'un cadenas dans la fenêtre du navigateur Internet.

Contrôlez qu'aucune fenêtre internet n'est ouverte, tapez vous-même l'adresse exacte fournie par la banque.

N'activez la fonction Bluetooth ou Wi-Fi que lorsque c'est nécessaire et désactivez-la dès la fin d'utilisation.

N'accédez pas à votre banque à distance depuis un ordinateur public ou connecté à un réseau Wi-Fi public.

Si la date de votre dernière connexion est affichée, vérifiez-la. Quand vous avez terminé, utilisez le bouton « déconnexion » et effacez l'historique dès que vous avez fini.

Enfin si vous avez supprimé des documents, n'oubliez pas de vider la corbeille.

Paiement avec la carte bancaire

Je n'utilise pas ma carte bancaire sur n'importe quel site!

Le B.A.-BA

Sur le Web, le choix de la boutique est primordial. Préférez toujours un site ayant pignon sur rue et assurez-vous que les conditions générales de vente, l'adresse et le contact (e-mail, téléphone) du siège de la société sont facilement accessibles.

Pour plus de sécurité

Vérifiez au moment de l'achat que le site est sécurisé. Un « s » doit figurer après le « http » dans la barre d'adresse du site. Cette garantie est symbolisée par un petit cadenas fermé, en haut de la fenêtre de paiement.

Autre règle universelle, pour réaliser un achat sur Internet, il faut saisir le cryptogramme de sa carte bancaire (les trois chiffres figurant au dos), mais à aucun moment votre code confidentiel à quatre chiffres. Pour bénéficier d'un niveau de protection encore plus élevé, débloquez auprès de votre banque le service 3D Secure. Ce protocole est déjà mis en place sur de nombreux sites (SNCF, Fnac…). Il consiste en l'envoi d'un code par SMS sur votre smartphone, à saisir au moment du paiement, afin de vous authentifier comme l'acheteur réel et de confirmer le montant de la transaction.

Renseignez-vous auprès de votre établissement bancaire des démarches sécurisées et gratuites pour payer en ligne en toute sécurité.

Ne communiquez jamais vos mots de passe en cas de sollicitation par e-mail.

Vérifiez avec attention l'adresse Web et le logo du message.

Vous remarquez des erreurs de syntaxe ou de fautes d'orthographe ? Le message est probablement un phishing. Si un doute subsiste, contactez le site officiel – et non celui du mail – avant de communiquer quelque information que ce soit.

Sur Internet, ne payez jamais rien pour débloquer un éventuel gain substantiel. On ne paye pas ce qui devrait être gratuit !

Paiement sécurisé

Comment ça marche ?

Pour rappel, avec le paiement en ligne, l'argent est stocké de manière sécurisée par un partenaire de paiement le temps de la finalisation de la transaction. Dès que l'acheteur confirme la réception de l'article, l'argent est débloqué et le vendeur est payé directement sur son compte bancaire (en moyenne sous 3 jours, selon les délais bancaires). Pensez aussi à vous manifester si vous ne recevez pas votre colis, à défaut, l'argent est automatiquement débloqué et le vendeur est payé directement sur son compte (en moyenne sous 3 jours, selon les délais bancaires). À aucun moment, il n'est donc question de SMS.

Que faire en cas de fraude à la carte bancaire ?

Qu'appelle-t-on une fraude à la carte bancaire sur internet ?

Plusieurs cas sont possibles. Parmi les plus courants :

- Je remarque sur mon relevé bancaire des achats en ligne dont je ne suis pas à l'origine,
- J'ai reçu un code de confirmation sur mon téléphone pour un achat que je n'ai pas fait,
- J'ai été averti par ma banque d'une tentative d'utilisation frauduleuse de ma carte bancaire sur internet.

Que faire si je suis victime d'une fraude à la carte bancaire sur internet ?

En priorité, je fais opposition à ma carte, auprès de ma banque qui me remettra un numéro d'opposition à conserver pour la suite de la procédure. Ensuite, je signale la fraude sur **service-public.fr.** A la fin de ce signalement, j'obtiendrai un récépissé, qui facilitera mes démarches de régularisation auprès de ma banque.

Comment faire ce signalement ?

Avant de démarrer la démarche en ligne sur service-public.fr également connue sous le nom de « Perceval », je prépare les informations dont j'ai besoin :

- **mon numéro d'opposition,**
- **mon numéro de carte bancaire,**
- **mes relevés bancaires.**

Pour accéder à la démarche en ligne sur service-public.fr, il faut obligatoirement que je m'identifie avec **FranceConnect**. Pour cela j'utilise un des comptes que j'ai déjà créé auprès des organismes proposés tels que les impôts ou Améli. Une fois connecté à la démarche en ligne, je fournis les informations sur les achats effectués à mon insu.

Ma demande sera traitée par la gendarmerie nationale et je recevrai sous quelques heures un email accusant réception de la déclaration. Le récépissé sera également disponible dans la partie « mes documents » de mon espace personnel service-public.fr.

Pourquoi signaler une fraude à la carte bancaire ?

En plus de simplifier mes démarches auprès de ma banque, mon signalement permet de faciliter les enquêtes

Assurances vie

ATTENTION AUX OFFRES FRAUDULEUSES

L'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Autorité des marchés financiers (AMF) constatent, depuis plusieurs années, une recrudescence des arnaques aux placements, crédits et assurances à la faveur d'un usage toujours plus grand d'internet, d'outils de communication mobiles toujours plus accessibles et d'un contexte de taux d'intérêt bas.

De plus en plus de publicités sur internet proposent des placements à forte rentabilité, qui se révèlent très risqués pour les consommateurs. Renseignez-vous sérieusement sur ces placements et ne vous laissez pas influencer par des promesses de gains rapides et importants !

Promesses d'argent

LA FRAUDE AU RACHAT DE CREDITS

Depuis quelque temps, la fraude au rachat de crédit s'intensifie. Dans ce scénario de fraude, des **escrocs se font passer pour un organisme de crédit.** Ils contactent les détenteurs de crédit avec la promesse d'un rachat à un taux imbattable. Prétextant les démarches pour une ouverture de dossier, les fraudeurs soutirent aux victimes toutes **les informations nécessaires** à l'ouverture d'un crédit en ligne. **Un nouveau crédit est alors ouvert** avec l'identité usurpée. La somme empruntée est versée à l'établissement de crédit sur le compte de la victime qui est ensuite recontactée pour transférer le montant vers un compte externe. Croyant finaliser l'opération de rachat de crédit, la victime ne se méfie pas et son argent disparaît dans la nature.

Des vérifications simples pour déjouer les arnaques

Conseil élémentaire

Pour déjouer ce type d'arnaque : toujours se méfier des offres trop belles pour être vraies. On vous promet un taux record et des délais de remboursement très longs, un accès au crédit sans aucune condition… En bref ce que ne vous proposera jamais votre banquier ou un spécialiste du crédit. C'est qu'il y a un loup ! D'autant plus si votre interlocuteur vous met la pression pour obtenir votre accord, invoquant une offre exceptionnelle à durée limitée.

Précaution

Comme toutes les autres chausse-trappes financières (phishing, arnaque aux placements…) ne communiquez jamais vos données personnelles et documents privés (pièces d'identité, carte de sécurité sociale, RIB…) après un échange téléphonique ou sur Internet à des personnes que vous entendez pour la première fois et que vous n'avez pas formellement identifiées. Surtout si vous n'avez rien demandé et s'ils se disent recommandés par un organisme que vous connaissez ou dont vous êtes client.

Pour lever tout doute, vous pouvez procéder à plusieurs vérifications sur des sites officiels. En premier que le courtier est un vrai professionnel ayant décroché le statut d'intermédiaire en opérations de banque et en services de paiement (IOBS). Ils sont tous recensés sur le site de l'Orias (https//www.orias.fr), le registre public des intermédiaires en assurance, banque et finance. La personne qui vous sollicite n'y figure pas ? Ne donnez pas suite.
Jetez aussi un œil sur la liste noire de l'Autorité de contrôle prudentiel et de résolution (ACPR), le gendarme des banques et des assurances, qui répertorie toutes les sociétés douteuses. Mais attention, même si elle est régulièrement mise à jour, les escrocs ont souvent un temps d'avance. Le nom ou le site de leur société peuvent ne pas encore y figurer.

Alertez enfin les autorités de cette tentative d'escroquerie sur le site de signalement du Ministère de l'Intérieur si vous avez été approché par Internet.

EN BREF

› Parlez à votre conseiller bancaire avant toute démarche de ce type.

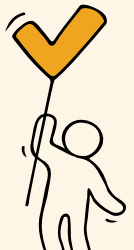
› Vérifiez toutes les informations concernant la société de crédit en question.

› Méfiez-vous d'emblée si un professionnel de crédit vous demande de rester discret sur le rachat. Ce n'est jamais bon signe.

› Les arnaques et les fraudes sont nombreuses. Les fraudeurs ont l'imagination fertile et sont de plus en plus organisés. Méfiez-vous des histoires trop belles, des gains d'argent faciles ou des abonnements à prix cassés.

› Fiez-vous à votre instinct avant tout et ne baissez jamais votre vigilance.

Si vous êtes victime d'une fraude qui a trait à votre argent directement, déposez plainte et parlez-en à votre conseiller bancaire dans les plus brefs délais.



LA FRAUDE AUX FAUX PLACEMENTS

1. Arnaque aux faux placements

L'Autorité des marchés financiers (AMF) et les professionnels du secteur de l'investissement appellent à la plus grande vigilance face à la forte augmentation de l'utilisation d'usurpations de noms d'acteurs ou de produits financiers pour faire souscrire aux épargnants des faux placements.

Le mode opératoire est généralement le suivant : vous remplissez un formulaire en ligne faisant miroiter des placements lucratifs et qui permet aux escrocs de collecter vos données personnelles.

Vous êtes ensuite appelé par un faux conseiller ou gérant se montrant très assuré et persuasif, vous pressant de vous décider rapidement pour souscrire l'investissement présenté comme une opportunité à saisir très vite.

En réalité, **l'investissement n'existe pas et vous perdez l'intégralité des fonds que vous avez virés !**

2. Arnaques à l'investissement

Places de parking

Portée par la crise sanitaire, une arnaque est en forte augmentation depuis le début de l'année 2020.

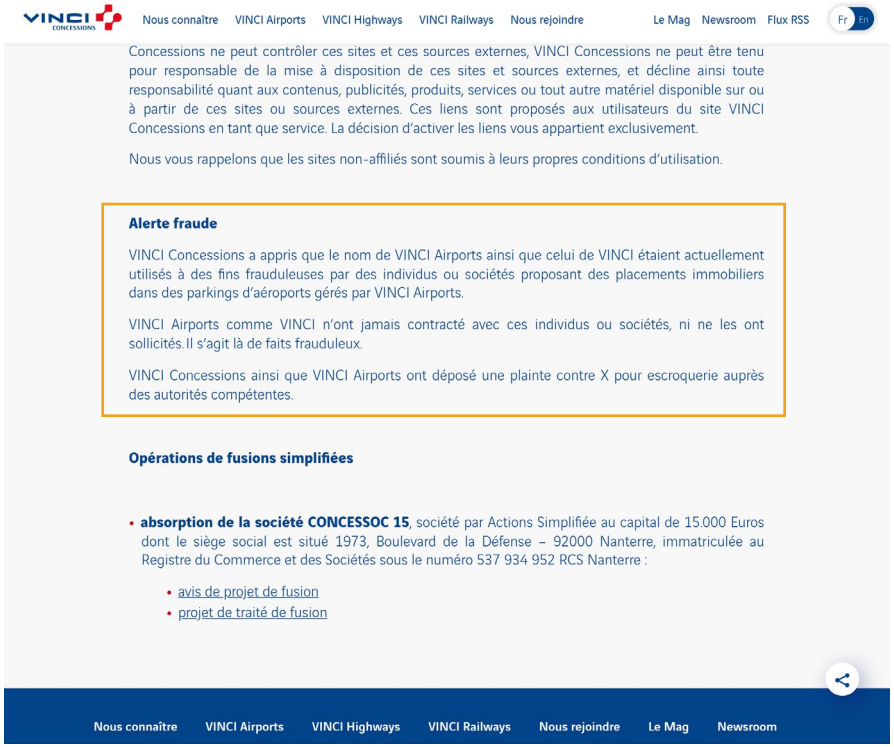
Dans cette période anxiogène, les escrocs misent en effet sur des valeurs refuges, telles que le whisky, l'or ou encore… des places de parking dans les aéroports européens.

Un site usurpe l'identité d'un conseiller en investissements financiers (CIF) afin de promouvoir une offre d'achat locatif via une place de parking dans un aéroport européen.

L'achat d'un tel espace permettrait de « *rapporter jusqu'à 14 % par an* ».

Il est demandé aux personnes intéressées d'entrer leurs coordonnées afin d'être rappelées.

Un faux CIF contacte l'épargnant et l'incite via un beau discours à acquérir une ou plusieurs places de parking, valant chacune 10 000, 15 000 €… pour les louer ensuite et obtenir une plus-value importante.



Une fois que vous aurez « investi » en versant de l'argent, il sera trop tard.

Vous n'aurez fait aucun placement et vous vous ferez voler votre argent, sans moyen de retrouver une trace de l'escroc qui se sera volatilisé.

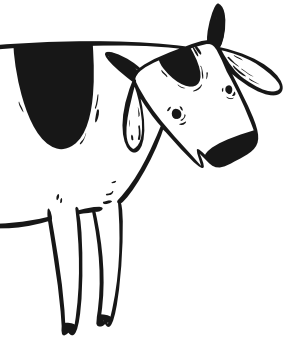
Si vous êtes victime d'une telle arnaque, portez plainte et alertez immédiatement votre banquier. Il sera malheureusement difficile de vous faire rembourser, les banquiers considérant que vous êtes bel et bien à l'origine du virement bancaire, réalisé de façon volontaire. Prévenez également les organismes partenaires du faux conseiller (banques, gestionnaires de parking, agents immobiliers…), qui pourront prévenir les autres consommateurs. Notamment, la société Vinci Concessions a publié un message sur son site Internet pour prévenir de tels agissements frauduleux.

Cheptels bovins

Investir dans une vache laitière. Voilà une opportunité sur laquelle les escrocs surfent allègrement depuis plusieurs mois. Un site Internet se présente comme une société intermédiaire entre investisseurs et éleveurs bovins (cheptel-agriculture.com, cheptelepargne.com, laitier-responsable.com, cheptel-patrimoine.com… la liste est longue). Pour l'achat d'une partie d'un cheptel bovin, donc de plusieurs vaches, il promet à chaque nouvel épargnant un rendement de 4 %, voire de 6 % à 12 %.

Deux options sont décrites pour récupérer les gains : revendre les vaches, censées avoir pris de la valeur, ou réinjecter les gains dans de nouvelles bêtes. L'élevage et l'entretien du cheptel sont supposés être réalisés par un agriculteur. « *Cet investissement est un investissement responsable, celui-ci permet de soutenir l'élevage agricole et vous permet un rendement entre 4 % et 5 %, nettement supérieur au livret A et LDDS (ex-LDD), de 0,75 % aujourd'hui* », peut-on lire sur l'un des sites, par ailleurs reproduit à l'identique sous différentes adresses url.

Pour toute demande d'information, l'internaute est invité à envoyer un message en laissant ses coordonnées pour être recontacté ou bien à appeler un numéro de téléphone. Certains sites permettent même de payer directement en ligne !



Sur la Ferme du Web, les clients peuvent investir sur une vache directement par carte bancaire.

Un commercial déverse ensuite au téléphone tout un discours à « l'investisseur », qui se décide à faire un virement – 10 000, 15 000 ou 20 000 €. Le piège se referme sur lui. La soi-disant société devient injoignable, les escrocs se sont envolés avec l'argent de leurs victimes, parti sur des comptes étrangers.

Toutes les informations délivrées sur ces sites sont fausses, du nom de la société aux promesses de rendement en passant par les supposés éleveurs ou investisseurs présentés dans un reportage. L'éventuel numéro de téléphone est temporaire et ne correspond pas au véritable numéro du malfaiteur. Les articles ou vidéos de presse relayés, eux, sont réels et basés sur de vraies informations, mais utilisés à des fins frauduleuses. Seul but des escrocs, qui surfent sur une proposition d'épargne alléchante : soutirer de l'argent à leurs victimes. Les chances de récupérer les sommes versées sont quasi inexistantes. Les personnes malveillantes agissant sous de fausses identités, les espoirs de retrouver son investissement disparaissent en même temps qu'eux.

Arnaque aux faux livrets à 7% de rendement

Les propositions de livrets d'épargne affichant des taux de rémunération très alléchants se multiplient sur Internet. Derrière elles, des escrocs utilisent des méthodes bien rodées pour soutirer un maximum d'argent aux victimes qui tombent dans leurs filets.

« Les Français profitent de ce livret jusqu'à 8 %. Êtes-vous éligible ? », « Ce nouveau livret d'épargne à 3,89 % disponible partout en France ! », « Un rendement 10 fois supérieur à celui du livret A » …

Si vous fréquentez les sites Internet de grands médias, sans doute êtes-vous déjà tombé sur ces bannières ou encarts publicitaires aux promesses réjouissantes. Mis en confiance par un environnement éditorial sérieux, certains se laissent tenter et en un clic, sont propulsés sur un site sur lequel ils peuvent « *tester leur éligibilité* » à ce placement miracle. Il suffit alors de rentrer nom, prénom, e-mail et numéro de téléphone pour qu'un message s'affiche : vous allez être recontacté par un conseiller.

Dernier exemple en date, celui débusqué sur un site d'information économique : un livret d'épargne à 3,89 % est mis en avant. On apprend qu'il apporte « *sécurité et rendement* » ainsi qu'une fiscalité clémente puisqu'il n'est « *soumis à aucune imposition* ». Mais ces arguments sont fallacieux puisque les livrets sécurisés affichent aujourd'hui des rendements peau de chagrin : 1 % net pour le livret A et le livret de développement durable et solidaire (LDDS) ou 2,2 % net pour le livret d'épargne populaire (LEP).

Espérer plus sans risque de perte en capital et sans aucun impôt à payer est donc tout simplement impossible. Un site qui propose une épargne à 3,89 % : passez votre chemin !

Arnaques financières diverses

Que ce soit sur Internet ou ailleurs, les arnaques financières fleurissent, pleines de promesses alléchantes visant à soutirer de l'argent à des épargnants. Offre exceptionnelle mais limitée dans le temps, rendements miraculeux, objets rares mais peu chers… Tous les arguments sont bons pour inciter les futures victimes à investir rapidement dans des produits à très haut risque, ou qui n'existent pas.

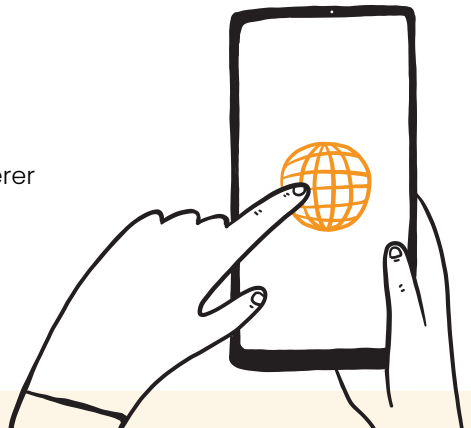
→ LE FOREX
(Foreign Exchange Market)

Le marché d'échange des monnaies mondiales – non régulé, à l'inverse du marché des actions –, est un terrain de jeu très prisé des « bandits de la finance ».

Sous une apparence sérieuse, des sites frauduleux mettent en avant des transactions séduisantes, avec des promesses de rendements très rapides, allant de 20 à 88 %. Ces sites illégaux, non autorisés à proposer du Forex, détournent les capitaux investis avant de disparaître.

⚠ Attention ! **tous les sites ne sont pas illégaux, mais ils restent dangereux.**

Certains malfaiteurs profitent de ces arnaques pour usurper l'identité des autorités financières (Autorité des marchés financiers (AMF), Autorité de contrôle prudentiel et de résolution (ACPR), Banque de France), ou même de Que Choisir, et proposer de récupérer les sommes perdues moyennant le paiement de taxes, qu'ils empochent avant de s'évaporer.



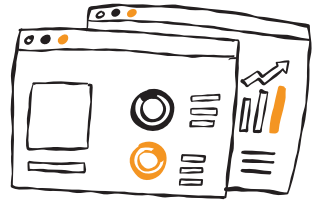
Autre source d'inspiration pour les arnaqueurs

→ LES PLACEMENTS ATYPIQUES

Encore une fois, ces derniers promettent des rendements prodigieux grâce à des investissements dans des produits alternatifs : diamants, vins, livres anciens, forêts… Or plus les rendements sont élevés, plus les risques le sont aussi, mais ces derniers ne sont jamais mentionnés.

Au contraire, les personnes malveillantes font valoir un moyen facile de s'enrichir. Dans le meilleur des cas, l'épargnant contraint à la promesse engagée sur une offre qui existe réellement n'augmente pas son capital.

Dans le pire des cas, il l'amoindrit, et la justice ne retrouvera pas la personne malveillante.



Le placement en diamants

Particulièrement en vogue aujourd'hui. Ce genre d'investissement est à proscrire : aucun des sites qui en proposent aujourd'hui (avançant des promesses de rendements à 8 %, un investissement sûr…) n'est autorisé à le faire. Les pertes peuvent atteindre plusieurs centaines de milliers d'euros.

Enfin, une autre arnaque, bien qu'ancienne, continue de causer des dégâts : **la vente pyramidale**, qui consiste à « recruter » des investisseurs en leur faisant payer des frais d'entrée généralement exorbitants ou en les incitant à faire des placements sur des fonds que l'on promet très rentables.

Avec ce système, l'argent versé par les derniers arrivés permet de rémunérer les investisseurs précédents. L'un des exemples les plus célèbres est la chaîne de Ponzi, un escroc qui a sévi dans les années 1920. Le modèle a été repris par Bernard Madoff, arrêté en 2008. Ce dernier payait les rendements des investisseurs avec les sommes placées par les nouveaux clients. Au moment de la crise financière de 2008, de nombreux clients ont voulu récupérer l'argent investi : le système s'est alors effondré, et l'escroquerie géante – près de 50 milliards de dollars ! – a été percée à jour.

3 ANNONCES

Offres d'emploi

Toujours gardez à l'esprit que si une offre d'emploi parait trop belle pour être vraie, elle est probablement douteuse. Méfiez-vous toujours des propositions trop alléchantes.

Les offres frauduleuses les plus courantes proposent :

- Un poste de magasinier à domicile / consignataire / réception de colis à domicile

- La garde d'enfants, d'animaux domestiques de familles résidant à l'étranger venant en France quelques semaines.

Il vous est proposé d'encaisser un chèque d'une somme importante avant même de vous avoir rencontré. Vous acceptez le chèque à titre d'avance sur salaire par exemple et vous devez reverser une partie à une tierce personne ou bien on vous apprend que le chèque reçu est erroné et il vous est proposé de rembourser la partie excédentaire. Il s'agit d'une arnaque ! Lorsque vous déposerez le chèque à la banque vous constaterez qu'il n'est pas encaissable et vous aurez remboursé une somme trop-perçu qui a été encaissée.

Les textes suivants n'ont pas été corrigés afin que vous puissiez constater les fautes d'orthographe, un des signes révélateurs d'arnaque.

Exemples de propositions frauduleuses :

1.

La société SDM DISTRIBUTION s'est forgée une renommée dans le Commerce International tant par son dynamisme et sa capacité d'écoute des partenaires que par sa rigueur et son sérieux dans les montages financiers accompagnant sa démarche commerciale.

Présent dans quatre régions du monde, la société SDM DISTRIBUTION propose à leurs clients, des solutions alliant une ample gamme de produits et des moyens de paiement adaptés à leur fonctionnement. Notre efficacité et notre flexibilité permettent d'offrir aux fournisseurs et aux clients des solutions sur mesure assorties de conditions financières compétitives, nos responsables commerciaux élaborent : Cependant, nous recherchons des Agents de conditionnement à domicile, des assistances aux différentes commandes en tant que Gestionnaire de stock afin d'intensifier notre activité. Toutes les charges concernant l'achat du matériel et les frais d'expédition du matériel seront pris en charge par la comptabilité de notre structure.

Cet emploi vous permet d'en avoir un autre, car lorsque vous êtes absent le/les transporteurs passent et ne vous trouvent pas, ils laissent un avis de passage afin de vous rendre à la poste pour récupérer le/les colis en instance de réception à la poste. Les profils les plus variés sont les bienvenus, quels que soient vos diplômes, votre niveau d'études ou votre expérience, faite nous parvenir votre CV à contact@smd-distribution.com si l'offre d'emploi vous intéresse afin de vous envoyer plus d'information concernant le poste à promouvoir. Aussi sachez que c\'est bien un travail rémunéré, et le salaire mensuel brut est de 1.400 euros. Une prime est accordée à chaque employé selon la disponibilité et la rapidité dans l'exécution de leur tâche.

Cordialement L'ÉQUIPE SDM DISTRIBUTION

2.

Bonjour, AX SERVICES ET DISTRIBUTION recrute des personnes, pour des postes de concierge livreur à domicile, En effet, certaines aptitudes sont nécessaires pour effectuer des opérations commerciales pour le compte de notre entreprise. Habilitée à recevoir nos commandes à leur domicile. LE POSTE DE CONCIERGE LIVREUR est un travail à temps partiel avec un contrat de travail inclut rémunéré 1300 Euros net/mois. Votre prestation consistera entre autre à recevoir et préparer les colis, imprimé et scanner des factures ou documents et diverses informations relatives aux livraisons qui vous seront confiées et les réexpédiers via des transporteurs avec qui nous travaillons déjà. Nous avons adopté cette méthode de travail afin de minimiser les frais inutiles de location d'entrepôts. Tous les frais de commande y compris les frais de transport depuis la livraison Jusqu'à l'acheminement des colis vers les différents clients sont prise en charge par notre entreprise. Faite nous parvenir un CV et un numéro de fixe ou portable par mail : NB: Vous devez disposer d'un ordinateur avec accès à Internet à domicile et d'une imprimante.

Bien a vous AX SERVICES ET DISTRIBUTION

3. Arnaque faux chèque

(...) je voudrais pour le début de notre collaboration vous confier une petite tache considérons cela comme une prestation de service et vous serai rémunérer pour cela. Je vous explique : Avant mon départ je devais être payée par un de mes client pour achat de plusieurs de mes produits en cosmétiques et parfums, c'est un client régulier et il a pour habitude de me payer par chèque mais vu mon départ un peu précipité j'ai pas pu récupérer le chèque chez lui et en plus de cela il voyage il va en croisade pour les fêtes avec sa famille samedi donc je pourrai plus le revoir a mon retour. Je reviens la dans une a deux semaines au plus, je suis joignable au 0680894220, j'espère que je peux vous faire confiance et je vous écris de suite. Je vous prierai alors de recevoir le chèque a ma place et a l'encaisser le temps que je revienne sur paris. Il le fera refaire en votre nom puis vous l'expédiera pas la poste. Je considère cela comme un premier test pour vous. J'espère que cela ne vous dérange pas et ne vous pose un problème. (..)

Cependant les auteurs d'arnaque à l'emploi peuvent être très imaginatifs dans leurs démarches.

Les escrocs identifient un demandeur d'emploi et lui proposent un job bien payé. Ce subterfuge a pour but de vous recruter en tant qu'intermédiaire pour une opération de blanchiment d'argent. Ces fausses propositions et offres d'emploi prennent le plus souvent toutes les apparences de la réalité et cherchent à attirer les candidats avec une rémunération et/ou une souplesse horaire particulièrement attractive(s).

Leur objectif est de soutirer de l'argent aux candidats, ou de leur dérober des informations personnelles sensibles (données bancaires, numéro de sécurité sociale, etc.) pour en faire un usage frauduleux.

Avec **12 millions de connexions mensuelles** dédiées à la consultation d'offres d'emploi, l'audience du portail de Pôle Emploi attire les escrocs.

Cela peut prendre la forme de mails frauduleux usurpant aussi l'identité de spécialistes comme Adecco, Monster, Randstad… En 2016, Pôle Emploi a supprimé **11 000 annonces frauduleuses** et fermé **4 800 comptes d'entreprises et recruteurs bidons** !

Des méthodes qui doivent vous alerter :

Après vous avoir mis en confiance, votre faux futur employeur se contente d'un **entretien d'embauche par téléphone ou visio-conférence** (via Skype ou autre messagerie). Il vous adresse une lettre d'embauche ou un contrat de travail bidon et exige de votre part des justificatifs d'identité, de domicile, un relevé d'identité bancaire, etc. Il a alors tout en mains pour usurper votre identité.

Avant même d'être embauché(e), vous recevez un premier chèque de salaire et d'un montant supérieur à la somme convenue ! Votre employeur prétend s'être trompé et vous demande de lui rembourser le trop-perçu. Ce que vous vous empressez de faire… avant que votre banque vous informe que son chèque présenté à l'encaissement est volé ou falsifié.

Comment vous prémunir ?

Cinq points qui doivent mettre en alerte une personne qui va se positionner sur une offre d'emploi

1

Vérifiez bien toutes **les informations et les coordonnées** présentes sur l'annonce. Vérifiez la présence de l'entreprise sur le web et sa réputation. Si vous ne trouvez rien sur cette société ou si vous tombez sur un site peu fiable, ne donnez pas suite.

2

Gardez à l'esprit qu'une entreprise normale ne vous demandera **jamais d'argent** pour quoique ce soit, ni ne vous en versera avant la signature d'un contrat de travail.

3

Méfiez-vous des offres trop belles c'est-à-dire qui proposent des salaires très attractifs et donc irréalistes.

4

Vérifiez la syntaxe et le style de l'annonce. Les vraies annonces sont rédigées par des professionnels des ressources humaines et ne comportent pas de fautes ou des tournures de phrases insolites.

5

Ne jamais fournir de pièces personnelles tant que l'on n'a pas eu un entretien en face-à-face ou que l'on a un accord de recrutement avec l'entreprise.

Et si vous pensez avoir reçu une proposition malhonnête, si une offre affichée en ligne vous paraît bizarre ou bien trop attractive, **alertez l'administrateur du site hébergeur ou votre conseiller Pôle Emploi** ainsi que son médiateur

mediateur.national@pole-emploi.fr

Si vous avez été abusé-e, le seul recours reste de déposer plainte pour escroquerie.

Annonces commerciales

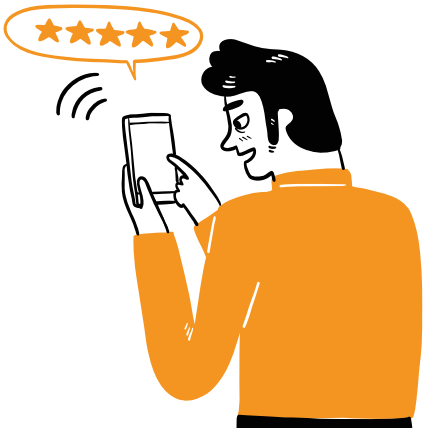
La pandémie de COVID-19 a conduit de nombreux consommateurs à se tourner vers le commerce électronique. Dans le même temps, de nombreuses fraudes et arnaques ont été mises en évidence par les services de contrôle : produits de faible qualité, voire dangereux ou qui ne sont pas livrés.

Faire ses courses, s'abonner à un magazine, louer un gîte… c'est parfois bien plus pratique et souvent moins cher sur internet qu'en boutique. Pas question pour autant d'en oublier toute vigilance ! Quelles sont les précautions à prendre ? À qui s'adresser en cas de litige ? Retrouvez dans ce guide les conseils de la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) pour acheter sur internet en toute sécurité.

Faux avis de consommateurs sur Internet

Pour choisir un restaurant, un hôtel ou tout simplement à l'occasion de l'achat d'un bien, vous êtes nombreux à consulter les avis de consommateurs accessibles en ligne : attention, ces avis ne sont pas toujours fiables.

La loi pour une République numérique a introduit des dispositions visant à sanctionner ces pratiques. Si vous avez un doute sur l'authenticité d'un avis, signalez-le. Et diversifiez vos sources d'information avant d'effectuer un achat !



→ On vous propose une place de concert gratuit si vous participez à un concours ?

De faux concerts ou spectacles promus sur des pages Facebook créées au Bangladesh, des sites de **streaming** bidon hébergés à Chypre, des fans piégés après avoir participé à des concours : des arnaqueurs donnent du fil à retordre aux artistes québécois, déjà malmenés par la pandémie.

Des personnes étaient intéressées ou avaient confirmé leur présence à l'événement. Sauf que le spectacle « gratuit » n'a jamais eu lieu. Et n'a jamais existé.

Des messages alarmants – « Plus que 2 minutes pour avoir des places » par exemple –, s'affichent. Préférez les sites officiels (Fnac, Digitick, Ticketmaster…) et renseignez-vous sur le site en question avant l'achat.

Ce genre d'évènements, qui visent bien souvent à soutirer des informations bancaires (voir onglet 2), prolifèrent sur Facebook, profitant de la COVID-19 pour s'immiscer dans une offre virtuelle abondante.

Voici une liste non-exhaustive des arnaques les plus courantes :

La durée de validité, les billets non nominatifs, les reproductions, les offres trop alléchantes.

→ Abonnements cachés

De plus en plus d'offres apparaissent sur Internet pour vous faire gagner des produits gratuitement ou vous les proposer à un prix très intéressant. Mais bien souvent se cache, dans les conditions générales de vente (CGV), un abonnement avec prélèvements mensuels. Attention aux offres trop alléchantes et lisez attentivement les mentions légales et les CGV !

La plateforme de VOD Disney+ a été lancée fin mars en France. Des escrocs ont usurpé l'identité de la marque et ont proposé, via des publicités sur les réseaux sociaux, de tester les services en avant-première pour un coût dérisoire. C'est la dernière version de l'arnaque à l'abonnement caché, qui existe depuis plusieurs années.

→ Publicité pour l'achat de billets

Une nouvelle vague de fausses annonces promotionnelles sévit actuellement. Disneyland, le Futuroscope ou encore Air France voient leur identité usurpée par des malfaiteurs qui vous font miroiter de prétendus gains via des messages envoyés sur votre smartphone. Cette arnaque est loin d'être inédite, les escrocs se faisant régulièrement passer pour divers organismes et marques, comme celle d'Ikea en 2019.

La supercherie démarre sur Whatsapp. Vous recevez un message sur l'application, vous proposant de gagner des cadeaux à l'occasion d'un anniversaire.

Appels frauduleux aux dons

Appels frauduleux aux dons, Fausses cagnottes - Vigilance !

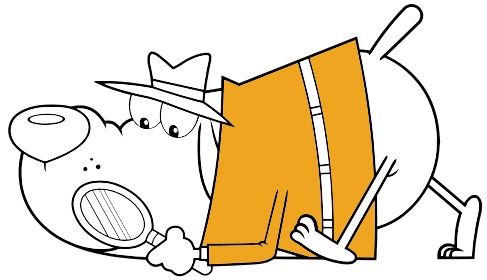
Dans le contexte de l'épidémie COVID 19, le risque d'escroquerie généré par des appels frauduleux aux dons s'est accentué. Que vous soyez acteur du financement participatif ou consommateur voulant contribuer à des actions de solidarité, soyez vigilant.

L'arnaque aux animaux de compagnie

Les arnaques aux animaux de compagnie sur internet sont de plus en plus nombreuses.

Les escrocs profitent de l'amour porté aux bêtes pour arnaquer leurs victimes.

Pourtant, les arnaqueurs suivent très souvent les mêmes discours et les mêmes méthodes. Voici quelques points qui vous permettront de démasquer les escrocs dans leur tentative d'escroquerie aux animaux de compagnie.



Quelques pistes

- Bien souvent, les arnaqueurs prétextent un don ou un prix au rabais à cause d'une mutation dans un autre continent, ou un manque de temps pour s'occuper de l'animal. Les annonces disent clairement avoir besoin de vous pour « sauver » l'animal en question.

- L'annonce presse très souvent l'acquéreur (la victime) à envoyer de l'argent rapidement. La situation est décrite comme urgente : la mutation est imminente par exemple. Tout cela a pour objectif de vous forcer à prendre une décision rapide, sur un coup de cœur.

- Les photos sont celles d'animaux de race à forte valeur ou d'animaux connus pour leurs attraits mignons, il s'agit particulièrement de chiot chihuahua, chaton persan, chiot husky, perroquet, etc. Le but est d'attendrir la victime, charmé par ces animaux mignons.

- Vérifiez l'email de vos échanges ainsi que le code indicatif du numéro de contact. Il parait peu probable qu'une société utilise une adresse email gratuite comme Gmail ou Yahoo mail par exemple. Cela signifie qu'il s'agit probablement d'une annonce factice. Quant au numéro de téléphone, si le numéro indique un pays étranger notamment le continent africain, prenez garde car beaucoup d'arnaques de ce type viennent d'Afrique.

- Vérifiez l'orthographe des échanges. Les arnaqueurs sont connus pour ne pas bien maîtriser la langue française et de nombreuses fautes dans leurs annonces sont parfois le signe d'une arnaque.

- Vérifiez les photos des animaux. Vous pouvez utiliser la recherche d'image inversée de Google pour voir si les images présentées ne sont pas présentes sur d'autres sites internet. Si les photos existent sur d'autres sites sans lien avec le premier, il s'agit probablement d'une annonce frauduleuse.

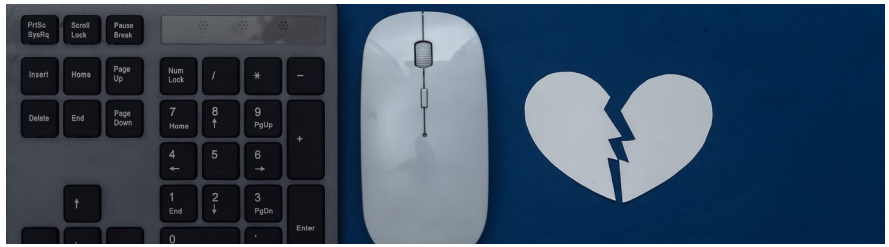
- Refusez de faire tout paiement via des modes de paiement non traçables comme Western Union, bons Transcash, cartes PCS ... Une fois le paiement effectué, vous ne pourrez plus le réclamer ! Pour ce type d'achat, le chèque est préférable car vous pourrez contester le paiement en cas de litige.

4 LES SENTIMENTS

La fraude sentimentale

ARNACOEURS, LES EXPERTS DE L'AMOUR EN LIGNE !

L'explosion des réseaux sociaux et des sites de rencontres sur le web révèle depuis peu le revers d'une médaille peu reluisante. Internet est devenu le terrain de chasse de personnes malintentionnées, à la recherche de proies en vue de leur extorquer de l'argent. Ils peuvent donc agir de deux façons, le chantage ou jouer avec les sentiments.



La face sombre du numérique

Parmi les escroqueries en ligne les plus répandues, les escroqueries sentimentales sont certainement **les formes de sextorsions** plus difficiles à éviter. Menées aussi bien sur les réseaux sociaux (Facebook, Instagram…) que sur les sites de rencontres (Tinder…), ces escroqueries en ligne occuperaient le deuxième rang du classement des crimes sur internet dans le monde en termes de coût (plusieurs centaines de millions d'euros), juste après le piratage d'emails en milieu professionnel.

Ils peuvent passer des heures à étudier les sites de rencontre et les réseaux sociaux à la recherche de la parfaite victime. Et une fois qu'ils l'ont trouvée, plus rien ne semble pouvoir les arrêter. Les escrocs contactent leurs cibles sur internet en parlant de leur vision de la vie ou de leurs loisirs préférés… bizarrement les mêmes que la victime ! Bien sûr, l'arnaqueur a su s'informer et faire les recherches nécessaires au préalable.

Tout se passe en ligne. C'est beaucoup plus facile pour les personnes esseulées à la recherche de l'âme sœur, mais aussi pour les arnaqueurs avides d'argent. L'autre problème, c'est que les victimes de telles escroqueries ressentent souvent une honte à en parler. D'où le faible taux de signalement et la difficulté à endiguer le problème.

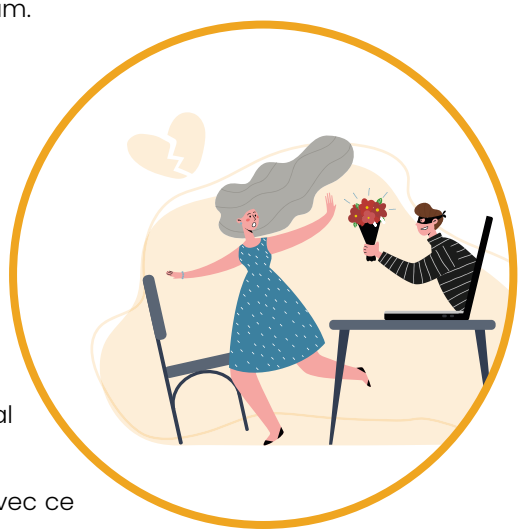
La manipulation est au cœur même du processus d'escroquerie sentimentale.

Le profil classique de la victime

La plupart des victimes des escroqueries sentimentales partagent le même type de profil. Ce sont généralement des femmes d'un certain âge, soit divorcées, soit veuves. Quant aux criminels qui s'attaquent à ces victimes fragiles, ils agissent en tant que véritables experts de la manipulation et sont loin d'être les princes charmants qu'ils prétendent.

Mais évidemment les hommes n'en sont pas à l'abri ! Ils charment leurs victimes jusqu'à échanger parfois des photos, ou des vidéos, mais celles qu'ils envoient sont des photos ou vidéos « empruntées », qui ne leur ressemblent jamais… et commence alors le chantage… ce sont des sextorsions ou arnaques à la webcam.

Quels sont les signes d'alerte ?



- Un nouveau contact en ligne exprime des sentiments forts à votre égard et veut vous parler en privé.

- Ses messages sont souvent mal rédigés et vagues.

- Son profil en ligne ne cadre pas avec ce qu'il/elle vous raconte.

- Il peut arriver que ce nouveau contact vous demande des photos ou vidéos intimes de vous.

- Il/elle gagne d'abord votre confiance. Cela peut prendre des semaines voire des mois. Puis, il vous demande de l'argent, des cadeaux ou vos données de compte ou de carte de crédit.

- Si vous n'envoyez pas d'argent, il/elle peut tenter le chantage. Si vous cédez, il ou elle exigera toujours plus.

- Il/elle recherchera toujours une excuse : la webcam ne fonctionne pas, il/elle ne peut entreprendre le voyage pour vous rencontrer ou il/elle a besoin d'encore plus d'argent.

La même démarche existe lors de l'organisation de voyages ou de rencontres à l'étranger.

QUELS SONT LES SIGNES ?

Un nouveau contact en ligne exprime des sentiments forts à votre égard et veut vous parler en privé.

Leurs messages sont souvent mal rédigés et vagues.

Leur profil en ligne ne cadre pas avec ce qu'ils vous racontent.

Il se pourrait qu'ils vous demandent des photos ou vidéos intimes.

Ils gagnent votre confiance puis vous demandent de l'argent, des cadeaux ou vos n° de compte / données de carte de crédit.

Si vous n'envoyez pas l'argent, ils peuvent tenter le chantage. Si vous cédez, ils exigeront toujours plus.

Exemples de phrases, de mots employés...

(Fautes d'orthographe, de syntaxe...)

« *Mon cœur* »
dans toutes ses phrases

« *Tu sais j'ai plus rien pour manger en ce moment sincèrement alors je veux que tu m'aide pour demain Mon cœur..* »

« *J'aimerais que tu le fais en Carte Pcs c'est encore mieux mon cœur* »

« *A toi maintenant de m'aider afin qu'on puisse arriver ensemble, si tu ne veux pas me comprends et m'aide aussi fais comme bon te semble Ok.* »

« *Mon cœur dit moi tu va acheter les coupons demain ou pas ?? J'ai besoin de ça tu comprends* »

« *Alors dit moi sincèrement si tu veux vraiment qu'on continue ou pas* »

« *Salu bel homme comment allez vous?* ».

« *Mon cœur tu sais bien que je tiens beaucoup à toi je fais de mon mieux afin qu'on puis être ensemble tu comprends* »

« *Mon cœur tu sais bien que moi je suis fou de toi j'ai vraiment besoin de toi dans mes bras en ce moment.* »

« *Mon cœur tu sais bien que je te rembourserai tout cela bébé car je t'aime fort tu es avec moi dans les moments difficiles sache que moi aussi je ne te laisserai jamais tombé chérie* »

QUE FAIRE ?

> Soyez très prudent/e concernant les données personnelles que vous partagez sur les réseaux sociaux ou les sites de rencontre.

> Tenez toujours compte des risques. Les escrocs sont présents sur les sites les plus réputés.

> Méfiez-vous d'emblée si un professionnel de crédit vous demande de rester discret sur le rachat. Ce n'est jamais bon signe.

> Ne précipitez rien et posez des questions.

> Enquêtez sur les photos et les profils de la personne pour voir s'ils n'ont pas été utilisés ailleurs.

> Soyez attentif/ve aux fautes d'orthographe et de grammaire, aux contradictions et aux excuses, comme une panne de caméra.

> Ne partagez pas de vidéos ou de photos personnelles, ni d'informations compromettantes ouvrant la porte au chantage.

> Si vous voulez convenir d'un rendez-vous pour vous rencontrer, dites à vos amis ou votre famille où vous allez.

> Méfiez-vous des demandes de fonds. N'envoyez jamais ni argent, ni données de carte de crédit ou de compte, ni copies de documents personnels importants.

> N'avancez jamais de l'argent par virement, transfert international, carte prépayée ou via cryptomonnaies à quelqu'un que vous ne connaissez pas. L'argent que vous transférez ainsi est extrêmement difficile à récupérer après coup.

> Ne transférez pas d'argent pour un tiers : le blanchiment d'argent est un délit.

Êtes-vous victime ?

- **Ne soyez pas gêné/e !** Les gens qui tombent dans le piège sont bien plus nombreux que vous ne le pensez.
- Stoppez immédiatement tout contact.
- Si possible, conservez tous les échanges (par exemple les chats), ainsi que toutes les preuves susceptibles d'aider à identifier les escrocs.
- Déposez plainte auprès des forces de l'ordre.
- Informez les gestionnaires du site internet sur lequel l'escroc vous a abordé/e. Donnez-leur le nom de profil de l'escroc, ainsi que d'autres détails susceptibles de les aider à mettre un terme aux tentatives de fraude.
- Vous avez déjà communiqué vos données de compte à l'escroc ? Contactez immédiatement votre banque.

Service info escroqueries

08 05 805 817

internet-signalement.gouv.fr

Portail officiel de signalement des contenus illicites de l'Internet

Site aux arnaques

internet-signalement.gouv.fr

Abus de confiance

L'abus de confiance est le fait pour une personne à qui a été remis de l'argent ou un bien, de détourner l'usage de ce bien à son profit ou pour un usage frauduleux. La victime peut porter plainte et demander réparation de son préjudice. L'importance de la sanction dépend de la vulnérabilité de la victime et du statut de l'auteur des faits.

Pour que l'abus de confiance soit reconnu, il faut :

→ Un accord préalable

Il faut nécessairement un accord préalable (écrit ou oral) entre la victime et l'auteur de l'infraction. Cet accord peut, par exemple, prendre la forme d'un contrat de travail, de prêt ou de mandat.

→ Une remise de la chose

La remise de la chose (somme d'argent, chéquier, ...) doit avoir été volontaire (dans le cas contraire, les faits pourraient alors être qualifié de vol). Inversement, l'auteur de l'infraction doit avoir eu conscience du caractère temporaire de la détention et donc du fait que la victime ne lui a pas cédé la propriété de la chose.

→ Un détournement

Lorsque ces conditions sont réunies, la personne se rend alors coupable de l'infraction lorsqu'il réalise un détournement qui peut notamment apparaître sous la forme d'une non-restitution, d'une destruction, d'un don, d'une vente, d'une détérioration... Par ses actes, l'auteur de l'infraction s'approprie la chose alors que celle-ci ne lui appartient pas. La victime en subit un préjudice qui peut être matériel ou moral.

Exemple : La carte bancaire a été remise à l'aide-ménagère pour effectuer les courses. Elle en profite pour effectuer des achats pour son compte personnel.

A noter

Aucune poursuite pénale ne peut être engagée pour l'abus de confiance entre époux ou entre enfants et parents (immunité familiale) sauf s'il s'agit d'un objet ou un bien indispensable à la vie courante (carte d'identité, carte bancaire, titre de séjour...) détourné et que la victime est son époux, son parent ou son enfant.

Différence entre le vol, l'escroquerie et l'abus de faiblesse

• L'abus de confiance se distingue de l'escroquerie.

Pour l'abus de confiance, il n'y a pas de fraude initiale. L'auteur des faits possède un réel droit sur le bien concerné. Pour l'escroquerie, l'auteur fait croire qu'il possède un droit sur le bien (par exemple, l'auteur des faits retire de l'argent sur le compte de la victime avec une fausse procuration).

• L'abus de confiance se distingue du vol.

Dans un abus de confiance, la victime a volontairement remis le bien à l'auteur des faits ou a permis à l'auteur de disposer de ce bien. Il y a vol si le bien a été pris par l'auteur des faits sans aucun consentement et sans remise volontaire de la victime.

• L'abus de confiance se distingue aussi de l'abus de faiblesse.

Il y a abus de faiblesse quand l'auteur profite de l'état de faiblesse d'une victime pour qu'elle fasse un acte dont elle ne mesure pas toutes les conséquences. L'état de faiblesse se caractérise par exemple par l'âge, le handicap ou la grossesse d'une personne.

Comment l'éviter ?

- Demander les tickets de caisse
- Vérifier ses relevés de compte bancaire régulièrement

Recours de la victime

a / Plainte au pénal

- La victime peut déposer plainte pour abus de confiance.

- La plainte doit être déposée dans un délai de 6 ans après la découverte des faits. La date de découverte des faits est celle où la victime dispose des éléments pour constater le détournement de ses biens. Par exemple, lorsqu'elle constate que l'argent n'est pas sur son compte.

- Cependant, il n'est pas possible de porter plainte plus de 12 ans après les faits même en cas de découverte tardive.

b / Autres actions

- Si l'auteur des faits possède une procuration, la victime peut y mettre fin.

- Elle peut aussi faire opposition aux virements au profit de l'auteur des faits. Il est impossible de demander le blocage de sa carte bancaire ou de ses chèques.

5 INTERNET

L'une des meilleures façons de se prémunir contre les pertes de données suite à une attaque, est tout simplement de les sauvegarder assez régulièrement. Vous pourrez ainsi retrouver vos fichiers si vous ne parvenez plus à y accéder sur votre ordinateur. Un disque dur externe ou une clé USB (que vous débrancherez une fois l'opération de sauvegarde terminée) feront très bien l'affaire.

Vous voulez écrire ce que vous voulez et où vous voulez sur le web ?

Ce qui est bien, c'est que vous êtes anonyme sur la toile....

Faux ! Il est très important de contrôler la diffusion d'informations personnelles. Internet et les réseaux sociaux sont loin d'être ce lieu d'anonymat qu'on imagine. Évitez de fournir vos coordonnées ou d'autres données sensibles dans les forums ou sur des sites n'offrant pas toutes les garanties requises. Un conseil : le symbole https:// au début de l'adresse web et l'image d'un petit cadenas est gage de site web certifié et sécurisé, mais dans le doute, mieux vaut s'abstenir.

Antivirus ou pare-feu

Aucun ordinateur n'est pas imprenable. Ne facilitez pas la tâche aux hackers. Mieux vous serez protégé, plus rude et dissuasive sera la tâche pour les personnes malveillantes. En informatique, le pare-feu permet de limiter un certain nombre de connexions entrantes et sortantes. Si malgré tout, le pirate trouve une faille dans votre ordinateur, un antivirus peut l'empêcher de nuire.

La clé WiFi

Il existe plusieurs types de clés WiFi. La clé WEP est la plus courante. Qu'est-ce que la clé WEP ?

Clef Wep ou Wap c'est une sécurité WiFi de la box. Les chiffres sont en bas de la box. Il faut l'enregistrer quand on paramètre la box. C'est la clé de sécurité. La clé WEP est fourni par le fournisseur d'accès. Souvent, elle se trouve sous la BOX.

Elle reste habituellement le choix par défaut des fournisseurs d'accès. Mais c'est également la moins sécurisée. Les clés WEP peuvent être décryptées par des pirates en moins de cinq minutes, contre une quinzaine d'heures pour une clé WPA 2.

Pour basculer vers cette dernière, saisissez « 192.168.1.1 » sur la barre d'adresses de votre navigateur Internet ou accédez directement aux paramètres de votre WiFi depuis votre compte personnel en ligne auprès de votre fournisseur d'accès.

Mails, rançons

a. E-mail

Un e-mail vous semble suspect ?
alors répondez aux questions suivantes :

Est-ce inattendu ?

Vous recevez sans raison un message de correspondant ; vous n'avez rien acheté, vous n'avez plus eu de contacts depuis longtemps, etc. C'est une raison valable pour être vigilant et vérifier l'authenticité du message.

Est-ce urgent ?

Gardez votre sang-froid ; avez-vous réellement reçu une première sommation de payer ? Connaissez-vous vraiment ce prétendu « ami en difficulté » ?

Connaissez-vous l'expéditeur ?

Contrôlez l'adresse e-mail, vérifiez si elle contient des fautes d'orthographe. Mais attention, une adresse e-mail légitime n'offre pas toujours de garanties quant à la véracité de l'e-mail.

La question qui vous est posée vous semble-t-elle étrange ?

Une instance officielle ne vous demandera jamais de transmettre par e-mail, SMS ou téléphone votre mot de passe, vos coordonnées bancaires ou vos données personnelles.

Où mène le lien sur lequel on vous incite à cliquer ?

Placez votre curseur sur le lien sans cliquer. Le nom de domaine, c'est-à-dire le nom qui précède .fr, .com, .eu, .org et la première barre oblique « / », correspond-il réellement au nom de l'organisation ?

Est-ce que l'e-mail s'adresse à vous personnellement ?

Il vaut mieux se méfier des messages dont le titre général est vague ou dont le titre est votre adresse e-mail.

Le message contient-il beaucoup de fautes d'orthographe ou de grammaire ?

Même si les cybercriminels malins s'efforcent d'utiliser un langage correct, des fautes ou l'emploi d'une langue étrangère peuvent être le signe d'un message suspect.

b. Rançons

A quoi ressemble un cas typique de chantage à la webcam ?

La victime se rend sur un site de rencontre puis entame la conversation avec une jeune femme ou un jeune homme au physique attrayant. Après lui avoir posé quelques questions sur sa vie privée, cette personne l'invite à approfondir les échanges via une conversation vidéo plus intime. Quelque temps plus tard, un courriel ou un message Facebook apprendra à la victime que cette rencontre a été enregistrée. Le cyber-escroc menace de diffuser la vidéo de cet échange sur le compte Facebook d'un proche ou sur un site de partage de vidéos si la victime ne lui remet pas la somme de 200 euros sous 24h/48h.

Quels réflexes adopter ?

1. Ne répondez surtout pas à un cyber-escroc
Soyez parfaitement hermétique à toute tentative de chantage : ne communiquez aucune donnée personnelle, ne versez surtout pas d'argent quelle que soit la somme demandée.

2. Verrouillez immédiatement vos comptes sociaux

3. Signalez directement l'escroquerie sur la plateforme **www.internet-signalement.gouv.fr**

4. Renseignez-vous via le service Info Escroqueries au **0.805.805.817**.

Usurpation d'identité

L'usurpation d'identité est un délit pénal.

Comment vous protéger du vol de vos données personnelles ?

Pour protéger vos données privées de potentiels piratages, quelques règles de base sont à appliquer :

- Choisissez un mot de passe sûr en alternant les majuscules et minuscules, les chiffres etc.
- N'utilisez pas un mot de passe unique sur tous vos comptes, alternez-les en fonction des sites.
- Ne partagez pas vos mots de passe et prenez vos précautions lors de leur utilisation sur d'autres ordinateurs que le vôtre.
- Vérifiez l'authenticité d'un expéditeur avant d'envoyer des informations personnelles ou sensibles par mail.
- Evitez d'inscrire votre adresse mail principale sur des sites dont vous n'êtes pas certain de leur fiabilité.
- Soyez attentif à vos relevés de compte bancaire.
- Détruisez tout papier comportant des informations personnelles avant de le jeter.

Les dangers des réseaux sociaux

Protégez au maximum votre profil sur les réseaux sociaux de façon à ce que des étrangers ne puissent pas vous contacter ou dérober vos données ou vos photos pour escroquer d'autres personnes.

Les cybercriminels qui disposent de vos données à caractère personnel telles que votre lieu de résidence, votre nom complet, votre numéro de téléphone et votre adresse e-mail peuvent exploiter ces informations pour vous voler de l'argent. Forts de ces informations, ils essaient de gagner votre confiance. Ils se font passer pour quelqu'un d'autre : une banque, un membre de votre famille, un bureau d'encaissement, et vous convainquent de partager vos coordonnées bancaires ou d'effectuer un paiement.

Exemples

Une supercherie démarre sur Whatsapp. Vous recevez un message sur l'application, vous proposant de gagner des cadeaux à l'occasion d'un anniversaire par exemple.

Cliquer sur le lien inséré vous amène vers un faux site de l'enseigne usurpée. L'un de vos contacts (ami, famille, collègue…) vous alerte : « Désolé, je t'ai envoyé par erreur mon code de sécurité à 6 chiffres. Peux-tu me le transférer s'il te plaît. C'est urgent ! »

Mais en réalité, la personne à l'origine de ce message n'est pas celle que vous croyez. Car son compte a été piraté ! Les arnaqueurs ont ainsi récupéré votre numéro de téléphone mobile et sont en train d'installer votre compte WhatsApp sur un autre smartphone. Aussi, si jamais vous leur communiquez ce code de sécurité (qui est vraiment envoyé par WhatsApp), vous tombez dans le piège. Grâce à lui, ils vont s'emparer de votre compte auquel vous n'aurez plus du tout accès et se faire passer pour vous !

La boucle est bouclée : les « scammers » vont utiliser le même procédé pour tenter de piéger vos contacts de la même manière.

Avant votre départ en vacances

→ N'indiquez pas vos lieux de vacances !

Mieux vaut éviter de confier vos lieux et vos dates de vacances à l'ensemble de vos abonnés Instagram ou votre liste d'amis sur Facebook ou sur Snapchat ! Il est également déconseillé de citer la ou les personnes avec lesquelles vous faites vos bagages…
Enfin, évitez de partager une confirmation de billet de train ou d'hôtel dans vos stories, que ce soit une capture d'écran, une numérisation ou une photo.

→ Soyez discrets sur vos biens !

N'oubliez pas de dépublier la photo de la télévision dernier cri achetée la semaine passée ! Un cambrioleur peut directement identifier sa future victime selon les biens qu'elle possède. Vous pouvez généralement, sur les réseaux sociaux, supprimer les anciennes publications de votre mur en quelques clics.

→ Évitez d'indiquer votre domicile !

Ne facilitez pas la tâche des « enquêteurs » ! Faites une recherche associée en tapant sur un moteur de recherche « *Votre adresse + votre nom* », ne géolocalisez pas votre domicile, n'indiquez jamais votre adresse précise sur les réseaux sociaux ou demandez directement à un site de dépublier votre adresse postale.

→ Pendant votre séjour : Faites une pause photo !

Ne postez pas de photos qui pourraient révéler la durée de votre trajet domicile-lieu de villégiature.

Peut-on faire confiance aux informations sur le web ?

Avec la pandémie et le confinement les arnaques se sont révélées quant à la vente des masques et du gel, leur qualité n'étant pas prouvée ou nulle.

Les sites spécialisés dans le domaine médical affichant le logo HONcode (Health On The Net Foundation) sont en général les plus fiables. Cela signifie qu'ils adhèrent à une charte qui les engage à respecter certaines règles, notamment en terme de vérifiabilité de l'information. C'est notamment le cas des sites Ameli-santé ou Allodocteur. La liste complète est disponible sur **hon.ch** on accède là à une information de santé fiable, transparente et éthique.

www.hon.cf/fr

6 COMMENT RECONNAÎTRE UNE ARNAQUE ?

Il s'agit souvent de fausses promesses vous faisant miroiter de gros gains d'argent.

Quelques exemples

• Vous êtes le grand gagnant d'une loterie à laquelle vous n'avez pas participé ;

• Vous avez l'opportunité exclusive d'intégrer un système pour gagner facilement et sans effort beaucoup d'argent ;

• Vous bénéficiez d'une commission élevée en aidant à mettre de l'argent en sûreté (héritage, capitaux, etc.) ;

• Vous êtes sélectionné pour investir votre argent sans risque avec, à la clé, un rendement élevé garanti.

1. Il ou elle est aimable, beau parleur et vous fait croire qu'il ou elle vous veut du bien. Ou, au contraire, il ou elle se montre agressif-ve, menaçant-e, vous harcèle.
2. Leurs lettres et leurs brochures peuvent vous sembler très professionnelles.
3. Il ou elle est convaincant-e.
4. Il ou elle a réponse à tout et ne renonce pas facilement lorsque le contact est établi.
5. Il ou elle vous pousse à vous décider immédiatement en vous offrant toutes sortes d'avantages supplémentaires.

Après avoir gagné votre confiance, il ou elle vous demande :

6. de verser une avance pour financer les frais administratifs, les taxes, etc. ;
7. de communiquer vos données bancaires, votre numéro de carte de crédit ou d'autres informations personnelles (numéro de carte d'identité) ;
8. d'appeler un numéro payant de type 0900 ou 0903, où vous n'obtiendrez finalement que de faux services ;
9. de télécharger un logiciel, soi-disant gratuit, mais qui s'avère être un abonnement payant à un fournisseur de services sur internet ;
10. d'acheter quelque chose pour accroître vos chances de remporter un prix plus important ;
11. de payer cash et de passer par un intermédiaire non-bancaire afin de leur transférer l'argent.

Quels sont les bons réflexes à adopter pour vous protéger ?

• Demandez-vous tout d'abord s'il est logique qu'un inconnu vous promette monts et merveilles.

• Prenez ensuite le temps de vérifier les coordonnées de votre interlocuteur. Les escrocs utilisent souvent un numéro de boîte postale comme seule adresse de contact, voire un GSM avec carte afin de ne pas être identifiés.

• Ne communiquez aucune donnée personnelle sans avoir vérifié à qui vous avez affaire.

• Ne donnez pas, ne versez pas et ne transférez pas d'argent à un inconnu ou à un intermédiaire financier sans savoir s'il dispose des autorisations nécessaires.

• Si l'on vous demande d'être discret, cela risque fort d'être une arnaque. Parlez-en autour de vous (amis, famille) et demandez conseil à un spécialiste ou à une personne de confiance.

• Utilisez les transactions sécurisées sur les sites d'enchères et refusez de traiter directement avec un vendeur.

Si vous êtes victime d'arnaque, portez plainte au commissariat ou à la gendarmerie. Même si les chances de récupérer vos gains sont minces, plus les autorités sont averties, plus les chances de stopper le réseau d'escrocs qui se cache derrière ces agissements s'agrandit.

Conclusion

Ce guide des arnaques a été pensé à l'usage des seniors en particulier mais peut être utile à chacun d'entre nous quel que soit son âge.

Il n'est pas exhaustif car l'imagination des escrocs et des arnaqueurs est sans limite.

Il ne se veut pas anxiogène, mais simplement informatif dans des domaines variés que notre groupe de travail a définis. Nous espérons qu'il vous aura permis de découvrir, de comprendre les mécanismes de l'arnaque et de vous alerter sur les méthodes utilisées.

S'il ne devait rester qu'une seule règle c'est celle-ci « soyez vigilant » mais surtout continuez à profiter pleinement de la vie.

LEXIQUE

Abandonniste : Ce terme désigne généralement le visiteur d'un site marchand qui quitte le site sans avoir commandé alors qu'il a mis au moins un article dans son panier ou caddie.
En dehors du contexte e-commerce, le terme d'abandonniste peut également être utilisé pour des visiteurs ayant montré par leur comportement de visite qu'ils éprouvent un intérêt plus ou moins fort pour une offre mais qui n'ont pas opéré la conversion (appel, formulaire, inscription, etc.).

Backdoor : logiciel qui permet au pirate de prendre le contrôle de l'ordinateur.

Bitcoin : C'est l'une des cryptomonnaies.

Chat : (ou tchat) : Système qui permet à deux ou plusieurs personnes de discuter virtuellement par écran interposé, (par écrit), sur internet ou via un logiciel adéquat.

Cryptomonnaie : Monnaie virtuelle stockée sur un support électronique qui permet à une communauté d'utilisateurs les acceptant en paiement de réaliser des transactions sans avoir à recourir à la monnaie légale. Depuis le 1er janvier 2019, le terme juridique et fiscal consacré dans la loi est celui d'actif numérique.

Dropshipping : C'est une forme de e-commerce par laquelle le site vendeur ne possède pas de stocks et fait livrer le client final directement par son fournisseur sans, le plus souvent, que le client ne le sache.

Hacker : C'est un spécialiste d'informatique, qui recherche les moyens de contourner les protections logicielles et matérielles. Il agit par curiosité, à la recherche de la gloire, par conscience politique, contre rémunération, ou bien par vengeance ou envie de nuire.

Hameçonnage (phishing en anglais) : C'est une technique qui consiste pour le fraudeur à se faire passer pour un organisme qui vous est familier (banque, administration fiscale, caisse de sécurité sociale…), en utilisant son logo et son nom et à vous envoyer un courriel dans lequel il vous est demandé de « mettre à jour » ou « de confirmer suite à un incident technique » vos données personnelles (comptes d'accès, mots de passe…) et/ou bancaires.

Illectronisme : C'est la difficulté, voire l'incapacité, que rencontre une personne à utiliser les appareils numériques et les outils informatiques. Le terme illectronisme transpose le concept d'illettrisme dans le domaine de l'informatique.

Keylogger : logiciel spécialisé pour espionner les frappes au clavier, il peut recueillir les mots de passe, les codes de carte bancaires, etc.

Malware : Terme générique qui désigne tout type de logiciel malveillant conçu pour s'infiltrer dans votre appareil à votre insu utilisé : virus informatique, vers, cheval de Troie, ransomware, spyware, adware, scareware, etc. Il existe de nombreux types de malwares et chacun poursuit ses objectifs malfaisants selon une approche différente. Cependant, toutes les variantes de malwares ont deux caractéristiques communes : elles sont sournoises et elles vont à l'encontre de vos intérêts.

Phishing : voir hameçonnage.

Scammer : C'est un arnaqueur qui prétend être en Afrique (souvent le Nigéria) ou dans un pays en voie de développement et qui vous sollicite par courriel pour récupérer des millions d'euros en échange d'un pourcentage.

Sextorsion : Ce délit consiste en l'extorsion via internet de faveurs sexuelles ou monétaires. Il se double le plus souvent de celui de chantage à la webcam.

Smishing : C'est une méthode d'arnaque semblable au phishing qui s'opère via le service de messagerie de téléphonie mobile SMS.

Spam : C'est une technique de prospection consistant à diffuser massivement par courrier électronique des informations, souvent de nature publicitaire, non sollicitées par les internautes destinataires Le phishing et le scam sont des formes de spam.

Spyware : logiciel espion qui collecte les données personnelles et les envoie à un tiers.

Storie (ou story) : C'est une photo ou une courte vidéo que l'on poste sur son compte Snapchat, Instagram ou Facebook, et que les amis / abonnés peuvent consulter pendant 24H. Après cela, elle disparaît. ...

Streaming : Ce système permet la lecture d'un flux audio ou vidéo (généralement fourni par des plateformes qui proposent plusieurs films, séries ou morceaux musicaux) à mesure qu'il est diffusé. Le stockage des données est provisoire et n'apparaît pas sous la forme d'un fichier sur le disque dur d'un destinataire. Les données sont téléchargées en continu dans la mémoire vive, sont analysées à la volée par l'ordinateur ou le smartphone et rapidement transférées vers un écran ou un lecteur multimédia (pour affichage), puis remplacées par de nouvelles données.

Task-Force : C'est un groupe de professionnels choisis en fonction de leurs compétences et de leur capacités (jugées pertinentes et complémentaires), réunis spécialement pour l'exécution d'une tâche ou la conduite d'un projet.

Webcam : Caméra conçue pour être utilisée comme un périphérique d'ordinateur, qui permet une communication visuelle et sonore via Internet.

Whatsapp : (ou WhatsApp Messenger) est une application mobile multiplateforme qui fournit un système de messagerie instantanée chiffrée de bout en bout aussi bien via les réseaux de téléphonie mobiles que par Internet. WhatsApp permet, comme on le fait pour un SMS, d'envoyer un message – texte ou vocal – à un ou plusieurs contacts, gratuitement, dans le monde entier et en utilisant un réseau 3G, 4G ou Wi-Fi. L'émetteur du message et tous les destinataires du message doivent être utilisateurs de l'application. Les conversations audio et vidéo sont également possibles à concurrence de huit personnes.

SOURCES

› https://www.service-public.fr/

› https://www.service-public.fr/particuliers/vosdroits/F31324

› www.economie.gouv.fr

› https://www.economie.gouv.fr/particuliers/renovation-energetique-arnaques#

› https://www.quechoisir.org

› https://www.orias.fr

› https://defense-des-consommateurs-ooreka.fr

› Insee

› Observatoire national de la délinquance et des réponses pénales

› Matmut

› https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-choisir-un-bon-mot-de-passe

› https://lesclesdelabanque.com/web/Cdb/Particuliers/Content.nsf/DocumentsByIDWeb/9W8AGL/$File/Guide-securite-04-banque-a-distance.pdf

› https://fr.statista.com/themes/3222/les-fraudes-bancaires-en-france/#dossierSummary

› https://www.airtransportanimal.com/faq/comment-reperer-arnaque-animaux

› https://www.leparisien.fr/societe/salu-bel-homme-sa-va-sur-twitter-le-fleau-des-arnaques-sentimentales-30-11-2019-8206344.php

Service Action Sociale
de la communauté de communes du Pays de Mormal

18, rue Chevray
59530 LE QUESNOY
Tél. : 03.27.09.04.60
contact@cc-paysdemormal.fr
www.cc-paysdemormal.fr