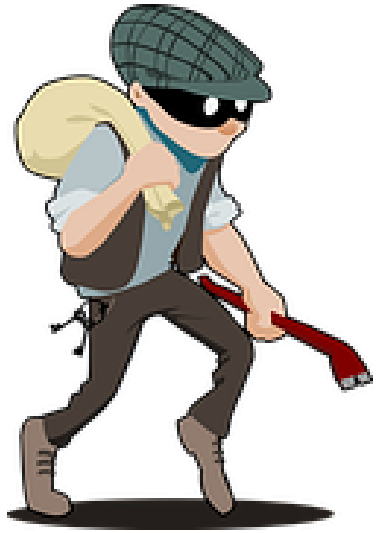
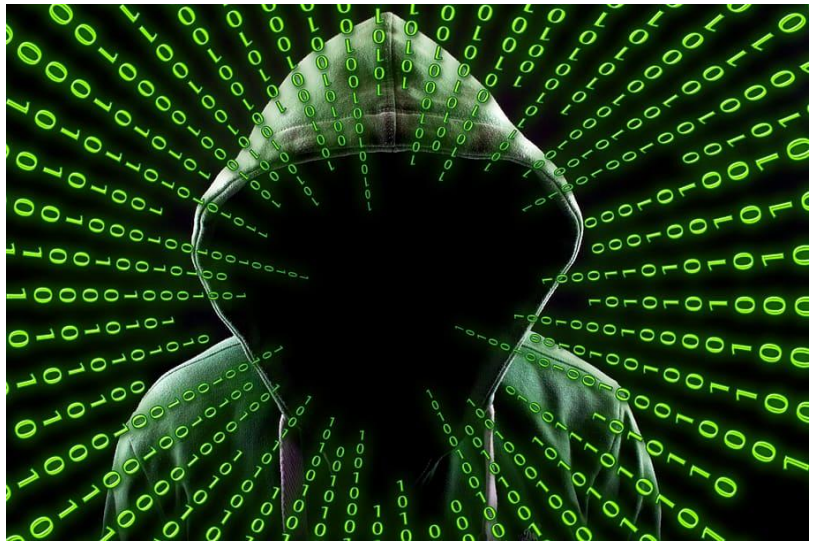
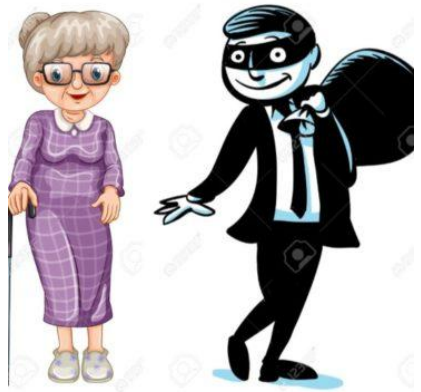
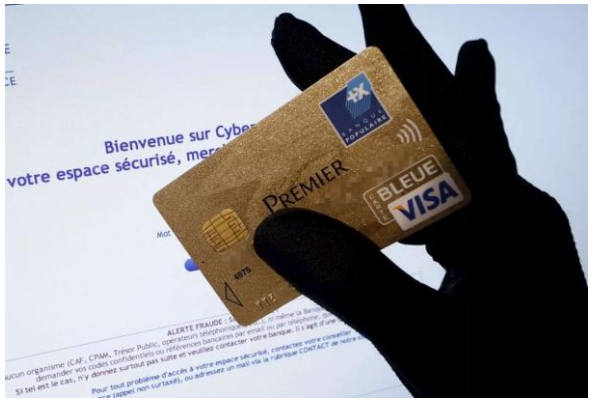






Arnaques bancaires :
Et si vous étiez la prochaine victime?



AFST
LES SENIORS DU TOURISME

Se faire arnaquer ne fait pas de vous un pigeon

- Un jour, quelqu'un a cliqué.
  Un jour, quelqu'un a répondu à un mail un peu trop urgent.
  Un jour, quelqu'un a cru qu'un prince exilé avait vraiment besoin d'aide.

Et devinez quoi ?
Ce quelqu'un… c'est des millions de personnes.

- Même des gens intelligents.
  Même des gens prudents.
  Même des gens qui savent très bien que **"vous avez gagné un iPhone"** sans participer à rien, c'est louche.

Les arnaques sont conçues par des professionnels de la manipulation.
Leur métier, c'est d'exploiter la confiance, la fatigue, la pression, l'émotion.
Votre métier, ce n'est pas d'être expert en escroqueries 24h/24.

👉 Se faire arnaquer, ce n'est pas une preuve de naïveté.
👉 C'est une preuve que vous êtes humain.

La honte appartient aux fraudeurs.
Pas aux victimes.

Alors on respire, on apprend, on en parle…
Et on laisse les escrocs faire le walk of shame à notre place.

Heureusement qu’on ne connait pas toutes les arnaques

Parce que sinon…

- On dormirait avec un casque en aluminium.
  On jetterait l’ordinateur par la fenêtre.
  On paierait en coquillages.
  On répondrait au téléphone en chuchotant :
  « Qui est là ? Donnez le mot de passe familial. »

La bonne nouvelle ?
On n’a pas besoin de vivre barricadés pour être protégés.

- On n’a pas besoin de connaître toutes les arnaques.
  On a juste besoin de reconnaître les plus fréquentes…
  et d’adopter quelques réflexes simples (promis, pas besoin d’un diplôme en cybersécurité).

Dans les prochaines minutes, nous allons voir:

Les arnaques les plus courantes

Comment elles fonctionnent

Et surtout, comment les déjouer sans devenir parano

- **Objectif :**
  Garder son calme.
  Garder son argent.
  Et garder son sommeil.

Parce que la sécurité, ce n’est pas vivre dans la peur.
C’est savoir où regarder… sans jeter son téléphone par la fenêtre.

Les fraudes bancaires

Les fraudes bancaires se multiplient, avec des méthodes devenant chaque jour plus élaborées : arnaques à la carte, fraude au virement, piratage de compte, prélèvements frauduleux, escroqueries… Les arnaqueurs, toujours plus inventifs, usurpent l’identité de votre banque ou d'autres organismes de confiance pour vous soutirer des informations sensibles et réaliser des opérations frauduleuses. Pour s'en protéger, il est essentiel de savoir reconnaître ces tentatives de fraude. Voici quelques-unes des fraudes les plus répandues et des astuces pour ne pas tomber dans ces pièges.

Les arnaques les plus fréquentes (1/3)

Le Phishing (ou hameçonnage)

- est une technique frauduleuse consistant à envoyer de manière massive un message semblant légitime (il peut s'agir de mail le plus souvent, ou de SMS) pour inciter la victime à cliquer sur un lien ou une pièce jointe potentiellement malveillants.

Escroquerie sentimentale

- Les escrocs approchent les victimes généralement sur des sites de rencontre, mais aussi via les médias sociaux ou par courriel afin de les amadouer, les séduire dans le but de leur soutirer de l'argent.

La fraude 419 (aussi appelée scam 419…)

- Un inconnu – ou quelqu'un se faisant passer pour un ami – demande votre aide pour transférer des fonds sur un compte étranger (par exemple, un héritage). Il vous promet une forte récompense à condition que vous lui fassiez d'abord parvenir une avance en argent. Bien entendu, la victime qui a versé son argent ne reçoit jamais un seul centime et n'entend plus parler de cet « ami ».

La fraude au faux conseiller bancaire

- La fraude au faux conseiller bancaire est un type d'escroquerie consistant à tromper la victime pour lui faire valider des opérations frauduleuses sur ses comptes.

Les arnaques les plus fréquentes 2/3

la fraude au QR code

- Une nouvelle fraude se répand en France : vous recevez par courrier une carte bancaire accompagnée d'un QR code à scanner pour l'activer. Pour éviter que des escrocs vident votre compte, sachez reconnaître une fausse carte

le smshing, le vishing et le quishing

- Le terme "phishing" est la contraction des mots anglais "fishing" qui signifie "pêche" et "phreaking" qui veut dire "piratage de lignes téléphoniques". On parle aussi de "hameçonnage".
- La même technique est aussi utilisée via des SMS, appelée alors "smshing".
- Quand il s'agit d'un appel vocal, on le nomme "vishing"
- Enfin, les fraudeurs ont adapté leurs méthodes en utilisant désormais les QR codes comme moyen d'attaque. c'est le "quishing". Cette variante du phishing émerge alors que le public devient de plus en plus vigilant face aux e-mails et SMS suspects.

La fraude au RIB

- Un escroc se fait passer pour votre **créancier** (bailleur, fournisseur, opérateur), il vous demande de faire vos virements sur un nouveau compte bancaire
- Les conséquences : une fois le virement effectué, l’argent est perdu.

Les arnaques les plus fréquentes 3/3

Les faux appels

- Ils font référence à des pratiques de manipulation psychologique à des fins d'escroquerie. Les arnaques au faux support technique, faux fournisseurs, faux banquiers, avocats ou commissaires aux comptes…l'attaquant cherche à abuser de la confiance, de l'ignorance et de la crédulité des personnes possédant ce qu'il souhaite obtenir. Chaque contact aura pour objectif un changement de coordonnées bancaires avant l'envoi d'un virement inhabituel ou de faire ouvrir un lien dangereux contenant un virus.

le ransomware et le chantage à la webcam

- Nous sommes tous "scotchés" à nos ordinateurs et il est bien compliqué aujourd'hui de vivre sans. Les escrocs l'ont bien compris. Les cyberattaques se développent et se multiplient tous les jours, notamment le ransomware et le chantage à la webcam

Le plus fréquent, le **fishing** – comment le reconnaitre

Un certain nombre d'indices ou de signaux doivent vous alerter. Vous pouvez regarder l'objet du message, l'action demandée, le ton employé et bien sûr le prétendu expéditeur. Un courrier électronique peut sembler provenir par exemple de votre banque, d'un site commercial bien connu, d'un site de paiement... Les prétextes sont nombreux.

L'objet du mail suspect ou frauduleux. Le mail de phishing peut avoir pour objet :

- "alerte sécurité"
- "confidentiel"
- "nous avons remarqué un problème sur votre compte"
- "votre compte a été restreint"
- "votre carte bancaire est suspendue",
- "activité inhabituelle sur votre compte",
- "message important de votre conseiller",
- "remboursement en votre faveur",
- "annulation de commande",
- "appel aux dons",
- "appel à l'aide",
- etc.

Le plus fréquent, le **fishing** – comment le reconnaitre

Une action urgente demandée

On vous demandera le plus souvent une action spécifique et rapide, dans votre intérêt. Il s'agira par exemple, de :

- mettre à jour ou confirmer vos données,
- changer votre code,
- régulariser une facture impayée,
- payer des frais de livraison supplémentaire pour récupérer votre colis,
- **…**

Les escrocs sont habiles et jouent sur l'affect et les sentiments humains, utilisant toute une palette d'**émotions**. Ces manœuvres frauduleuses reposent en effet sur la manipulation psychologique et utilisent l'envie de gagner de l'argent, la peur de perdre un droit ou de l'argent, la fierté d'aider les autres ou le besoin d'être solidaire… Le plus souvent, le mail de phishing est ainsi **alarmant**, demande une **action urgente**…

Comment se prémunir d'une escroquerie sentimentale

Soyez vigilant à ce que vous affichez comme information ou publiez sur les réseaux sociaux et les sites de rencontres.

- Les escrocs pourraient en effet utiliser ces informations pour mener à bien leur escroquerie.

Prenez le temps de connaître votre interlocuteur

- en lui posant de nombreuses questions et en évaluant la cohérence de ses réponses.

N'hésitez pas à demander l'avis de vos proches

- au moindre doute sur la sincérité de votre interlocuteur.

Effectuez une recherche inversée des photos de votre interlocuteur

- afin de savoir si ce sont bien les siennes. Les principaux moteurs de recherche proposent cette fonctionnalité.

N'envoyez jamais d'argent à une personne avec laquelle vous n'avez communiqué qu'en ligne ou par téléphone.

N'envoyez jamais de photos ou vidéos intimes à des contacts virtuels

- qui pourraient en profiter pour vous faire chanter.

Méfiez-vous si la personne promet de vous rencontrer mais prétexte toujours une excuse pour ne pas le faire,

- d'autant plus si cette situation perdure depuis des semaines, voire plusieurs mois.

Méfiez-vous si la personne tente de vous isoler de vos proches

Victime d’escroquerie sentimentale

- **Interrompez immédiatement toute relation avec l’escroc** même si celui-ci se montre menaçant par message ou par téléphone ou tente de vous faire chanter.
- **Conservez les preuves**, notamment les numéros de téléphone, les messages que vous avez reçus ou toute autre information qui pourront vous servir pour signaler l’arnaque aux autorités.
- **Déposez plainte** en fournissant toutes les preuves en votre possession.
  Pour ce type d’infraction, vous pouvez déposer plainte en ligne sur la plateforme THESEE accessible sur le site Service-public.fr.
  Vous avez également la possibilité de déposer plainte au commissariat de police ou à la brigade de gendarmerie ou encore par écrit au procureur de la République du tribunal judiciaire dont vous dépendez.
  Vous pouvez être accompagné gratuitement dans cette démarche par la fédération France Victimes au 116 006 (appel et service gratuits), numéro d’aide aux victimes du ministère de la Justice. Service ouvert 7 jours sur 7 de 9h à 19h.
- **Informez le site Internet sur lequel l’escroc vous a abordé** pour qu’il prenne les mesures nécessaires (suppression du profil de l’escroc, etc.).
- Si vous avez transmis des informations bancaires, **informez-en votre banque et surveillez régulièrement les opérations sur votre compte bancaire.**
- **Pour être conseillé dans vos démarches, contactez la plateforme Info Escroqueries** du ministère de l’Intérieur au 0 805 805 817 (appel et service gratuits). Le service est ouvert de 9h à 18h30 du lundi au vendredi.

Appels frauduleux aux dons – fausses cagnottes

- Dans le contexte d'une situation internationale instable , le risque d'escroquerie générée 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'essentiel

- Vérifiez que l'entité vous proposant le service est autorisée en consultant le site internet www.orias.fr.
- Vérifiez que la participation au financement du projet vous est proposée depuis le site internet d'une plateforme dédiée, régulièrement autorisée à exercer son activité, et sur laquelle vous vous êtes inscrit au préalable.
- Consultez la liste noire publiée par l'ACPR sur le site internet Assurance Banque Épargne Info Service – ABEIS (www.abe-infoservice.fr) et vérifiez que le site ou l'entité n'y figure pas.

Le vrai du faux

Comment signaler un faux mail de la gendarmerie ?

- Face à un faux mail de la gendarmerie, plusieurs plateformes officielles permettent de signaler ces tentatives d'hameçonnage. La plateforme Signal Spam constitue le premier réflexe pour signaler tout courriel de phishing suspect reçu dans votre boîte de réception. Vous pouvez également utiliser la plateforme Pharos (internet-signalement.gouv.fr) du ministère de l'Intérieur, spécialement dédiée au signalement des contenus illicites. Au moindre doute sur l'authenticité d'un message, vérifiez les dernières actualités et recommandations sur le site "gendarmerie.interieur.gouv.fr". Les véritables communications officielles ne demandent jamais vos identifiants de connexion ou numéros de compte par courriel.

Comment reconnaître un vrai mail des impôts ?

- Les courriels authentiques de l'administration fiscale respectent des standards précis facilement identifiables. Vérifiez l'adresse de l'expéditeur. Le nom de domaine gouvernemental constitue votre premier indicateur de fiabilité. Consultez les actualités et recommandations sur le site www.impots.gouv.fr L'administration ne vous demandera jamais vos coordonnées bancaires par courriel, que ce soit pour un remboursement ou un règlement. Les vrais mails des impôts ne contiennent pas de pièce jointe suspecte et leurs liens dirigent exclusivement vers le site officiel impots.gouv.fr. Lorsque vous recevez un courriel douteux, connectez-vous directement à votre espace personnel sur le site officiel pour vérifier si une action est réellement attendue de votre part.

Comment signaler un SMS frauduleux ?

- Face à un SMS frauduleux, transférez-le immédiatement au 33 700, la plateforme nationale gratuite de lutte contre les spams. Cette démarche simple permet aux opérateurs de téléphonie d'identifier et bloquer les numéros frauduleux. Vous pouvez également signaler ces tentatives d'escroquerie sur la plateforme Pharos via internet-signalement.gouv.fr, service officiel des autorités. Pour les cas les plus graves, n'hésitez pas à vous rapprocher de votre commissariat de police ou brigade de gendarmerie locale. Conservez une capture d'écran du message frauduleux avant de le supprimer : cela pourrait servir aux enquêteurs pour identifier les moyens frauduleux utilisés et protéger d'autres victimes potentielles.

Les risques

- L’ouverture d’une pièce jointe ou l’accès à un lien peuvent conduire à l’installation d’un malware ou ransomware(*) sur votre ordinateur.
- L’accès à un lien non sécurisé peut permettre le vol et/ou la fuite de données confidentielles comme vos identifiants/mots de passe, numéros et codes de cartes bancaires, etc.
- Ces données peuvent ensuite permettre au fraudeur de réaliser de l’ingénierie sociale : par exemple vous pouvez recevoir des appels de faux conseiller clientèle ou de faux service client, prétextant des paiements frauduleux ou des virements à annuler, qui seront en réalité validés par les codes que vous transmettrez.
- (*) chiffrement des données de l’ordinateur et réclamation d’une rançon contre le décryptage de ces données.

Les bonnes pratiques

- **Limitez la diffusion** de votre adresse email.
- **Nettoyez régulièrement votre ordinateur** à l'aide d'un antivirus à jour.
- **N'ouvrez pas les pièces jointes** d'un e-mail non sollicité ou douteux.
- **Ne cliquez pas sur les liens** sans vous être assuré de leur origine.
- En cas de réception d'un phishing, **signalez le mail** sur https://www.cybermalveillance.gouv.fr/ et supprimez le mail.
- En ce qui concerne l'accès à votre compte, **privilégiez l'accès direct** par l'application mobile ou la page d'accueil de votre banque en ligne (en saisissant l'adresse du site internet ou via votre favori), sans cliquer sur un lien transmis par mail ou sms.
- **Un conseiller clientèle ou téléopérateur** ne vous demandera jamais de données de connexion ou d'informations bancaires de type identifiant/mot de passe, numéro de carte bancaire, code de validation reçu par SMS, etc.
- **Parlez–en** autour de vous.

Les bonnes pratiques (suite)

Conseils pour détecter et se protéger des escroqueries

- **Vérifiez** toujours le nom et l'adresse de l'expéditeur ainsi que l'objet des mails que vous recevez. En cas de doute, n'ouvrez pas. Méfiez-vous tout particulièrement des mails avec des numéros de téléphone étrangers.
- **Méfiez-vous** des gains trop faciles et trop rapides, ils cachent généralement une escroquerie.
- Si l'un de vos amis vous réclame de l'aide en grande urgence, **essayez de vérifier** qu'il s'agit bien de lui en croisant plusieurs informations.
- **Ne communiquez jamais** vos données bancaires (code de carte bancaire, IBAN, identifiants et mots de passe…).
- **Ne surfez pas** sur les sites illégaux.
- **Protéger vos données** sur les réseaux sociaux avec des niveaux de confidentialités élevés.

Les recommandations

- **Vérifiez l'adresse email** : si l'expéditeur ou si l'adresse email vous semble suspecte, il s'agit certainement d'une tentative de Phishing.
- **Soyez prudents avec les liens et ne cliquez pas sans vous assurer de leur véritable destination** : positionnez le curseur de votre souris sur le lien, cela vous révèlera la véritable adresse du site sur lequel vous arriverez en cliquant. Sur un smartphone un appui long vous donnera le même résultat.
- **Soyez attentif au contenu et au niveau de langage** : faites preuve de méfiance si le message contient des fautes de grammaire ou d'orthographe (même si ce critère est de moins en moins déterminant). Méfiez-vous des demandes étranges, urgentes, illégitimes, alléchantes, ou vous demandant vos informations personnelles (codes, identifiants, mots de passe, N° de CB, etc.).
- **Méfiez-vous des pièces jointes** : n'ouvrez que celles que vous attendez et ne cliquez jamais sur un document qui vous parait suspect.
-

Je suis victime

- **Ne communiquez jamais le code secret de votre carte bancaire et ne la confiez pas à une personne qui viendrait la récupérer**, même si on vous a demandé de la découper préalablement.
- **Faites sans délai opposition à votre carte bancaire** en cas d'appel d'un faux conseiller, et a fortiori si des opérations frauduleuses ont été réalisés avec votre carte bancaire, pour empêcher toute utilisation malveillante ultérieure.
  Le numéro de téléphone d'opposition de votre banque figure sur son site Internet et sur ses distributeurs de billets. Vous pouvez également contacter par téléphone le serveur interbancaire d'opposition à la carte bancaire au 0 892 705 705 (numéro surtaxé), service ouvert 7 jours sur 7, 24h sur 24.
- Si les escrocs ont accédé à votre compte bancaire en ligne ou si vous le soupçonnez, **changez son code confidentiel/mot de passe d'accès au plus vite** ou demandez à votre banque de le réinitialiser.
- **Identifiez les opérations frauduleuses** réalisées par les escrocs avec votre carte bancaire et/ou les virements qu'ils auraient exécutés depuis votre compte bancaire ainsi que les comptes bénéficiaires leur appartenant.
- **Alertez votre banque** de l'ensemble des paiements et/ou virements frauduleux. Selon le cas, demandez-en le remboursement, la suspension ou encore le retour des fonds. Votre banque pourra exiger une copie de votre dépôt de plainte pour instruire votre demande.
- **Conservez les preuves**, notamment les numéros de téléphone, les messages ou mails que vous avez reçus, les ordres de virement, les relevés de paiements ou toute autre information qui pourrait vous servir pour signaler l'escroquerie aux autorités et vous être réclamée par votre banque.
- Si la fraude porte sur votre carte bancaire, **signalez les faits sur la plateforme Perceval**. Cette plateforme du ministère de l'Intérieur permet aux victimes de fraude à la carte bancaire de signaler en ligne l'escroquerie dont elles ont été victimes, et ce, même si elles ont été remboursées par leur banque. Votre signalement aidera les autorités à identifier les auteurs de ces fraudes. À noter que le signalement sur la plateforme Perceval ne se substitue pas au dépôt de plainte.
- **Déposez plainte** au commissariat de police ou à la brigade de gendarmerie ou encore par écrit au procureur de la République du tribunal judiciaire dont vous dépendez en fournissant toutes les preuves en votre possession.
  Vous pouvez être accompagné gratuitement dans cette démarche par une association de France Victimes au 116 006 (appel et service gratuits), numéro d'aide aux victimes du ministère de la Justice. Service ouvert 7 jours sur 7 de 9h à 19h.
- **Pour être conseillé dans vos démarches, contactez la plateforme Info Escroqueries** du ministère de l'Intérieur au 0 805 805 817 (appel et service gratuits).

Je suis victime

- Contactez dès que possible votre conseiller ou le service client de votre banque.
- Connectez-vous à votre espace banque en ligne ou mobile légitime et changez votre code d’accès, ou demandez à votre conseiller de le réinitialiser.
- Faites immédiatement opposition à votre carte bancaire sur votre application mobile, en appelant le numéro fourni par votre banque, ou à défaut le 0 892 705 705 (Ouvert 7 jours/7 et 24h/24 , numéro surtaxé) et conservez la référence de votre opposition. Si vous ne pouvez pas mettre en opposition votre carte rapidement, désactivez le paiement à distance ou les retraits sur votre appli mobile ou sur l’espace internet.
- Nettoyez votre ordinateur à l’aide d’un antivirus à jour.