

ARNAQUES FINANCIÈRES,

des escroqueries
classiques aux pièges
sur Internet

16 pages

**LIVRET
spécial
ARNAQUES**

Arnaques à domicile •
Fraudes sur Internet ou
par SMS • Testez votre
vigilance • Les bons réflexes
à adopter • Nos experts
du Net répondent.

Les pièges se multiplient

LES ESCROCS, TOUJOURS PLUS INVENTIFS, MANIPULENT LEURS VICTIMES AVEC DES MÉTHODES VARIÉES ET TERRIBLEMENT EFFICACES.

Les escroqueries, toujours plus nombreuses et diversifiées, mêlent aujourd'hui techniques traditionnelles et arnaques numériques sophistiquées. D'un côté, les classiques abus de confiance lors de démarchages à domicile ou parfois sur les foires et les salons qui continuent de prospérer. De l'autre, les pièges numériques tels que les e-mails frauduleux et les fausses notifications de remboursement par SMS qui se multiplient. En 2024, près de 9 Français sur 10 en ont été victimes⁽¹⁾. **Dans ce livret, plutôt que des recettes anti-arnaques, nous sommes partis de vos inquiétudes et de vos questions et nous les avons soumises à des experts.**

Car le but des escrocs est toujours le même, manipuler leurs potentielles victimes afin de mieux les tromper. Toujours plus ingénieux, les cybercriminels conçoivent aujourd'hui des arnaques difficiles à repérer. Personne n'est épargné, les malfaiteurs savent parfaitement s'adapter à l'âge et aux habitudes de chacun. ■

(1) Selon le rapport annuel d'activité de la plateforme Cybermalveillance.gouv.fr publié en mars 2024.



EST-CE QUE LES SENIORS SONT PLUS TOUCHÉS QUE LES PLUS JEUNES ?

Ultraconnectés, les adolescents, dès 11 ans, font preuve à tort d'un excès de confiance dans leurs usages numériques. Les jeunes adultes, attirés par des offres alléchantes sur les réseaux sociaux, sont, eux, particulièrement vulnérables aux escroqueries sentimentales, aux fausses offres d'emploi et aux arnaques à l'investissement. Selon l'AMF, 35 % des victimes de fraude à l'investissement en ligne avaient moins de 30 ans

en 2023⁽²⁾. Les seniors, quant à eux, restent les cibles privilégiées tant des fraudes classiques au démarchage à domicile que des arnaques numériques comme les faux e-mails ou SMS provenant soi-disant d'une administration ou de leur banque. Face à l'évolution constante de ces escroqueries, l'information et la vigilance deviennent plus que jamais cruciales. Des initiatives comme la stratégie nationale Educfi, opérée par la Banque de France, visent à renforcer les compétences financières de tout un chacun, quel que soit son âge, afin notamment d'être mieux armé face à de tels dangers.

(2) Selon le rapport annuel de l'Autorité des marchés financiers (AMF) de décembre 2023.

3 questions à

MARGUERITE COLLIGNAN,
DIRECTRICE DE
L'ÉDUCATION
FINANCIÈRE
À LA BANQUE
DE FRANCE



Crédit photo : Antoine Monégier du Sorbier.

1 Quelles sont les actions spécifiques menées par la Banque de France dans le cadre de la stratégie nationale Educfi pour sensibiliser et protéger les citoyens contre les arnaques et les fraudes ?

Afin d'améliorer les connaissances financières des Français, la Banque de France a par exemple mis en place un portail d'information www.mesquestionsdargent.fr destiné au grand public. Ce dernier couvre toutes les thématiques autour des finances personnelles (moyens de paiement, épargne, retraite...) avec notamment une rubrique dédiée aux arnaques afin de savoir les reconnaître et mieux s'en protéger en adoptant de bons réflexes. Mis à jour régulièrement par des experts de la Banque de France, le site permet de trouver des réponses claires et fiables.

2 Quelles sont les retombées concrètes de la stratégie Educfi ?

Tous les deux ans, la Banque de France fait réaliser une enquête afin d'évaluer les connaissances financières des Français. En décembre 2023, date du dernier sondage, une moyenne de 12,45/20 a été obtenue, ce qui est légèrement au-dessus de la moyenne de l'OCDE qui est de 12,2/20. Il s'agit d'un résultat très encourageant, même s'il reste encore des progrès à faire.

“La Banque de France a mis en place un portail d'information sur les questions d'argent.”

3 Dans un contexte où les escroqueries évoluent rapidement, comment les seniors peuvent-ils s'en prémunir efficacement ?

Sur le site www.mesquestionsdargent.fr, les seniors trouveront des explications claires sur les arnaques les plus courantes dont ils peuvent être victimes, comme les faux conseillers bancaires, l'usurpation d'identité ou les fraudes aux différents moyens de paiement. Par ailleurs, la Semaine de l'éducation financière se tiendra du 17 au 23 mars 2025. Comme chaque année, des animations, des ateliers et des tables rondes organisées dans toute la France traiteront notamment des arnaques financières.

**ADRESSE UTILE : RETROUVER FACILEMENT
LES SITES GRÂCE À CE FLASHCODE**
www.mesquestionsdargent.fr



Quel est votre niveau de vigilance face aux arnaques financières ?

LES ARNAQUES FINANCIÈRES N'ÉPARGNENT PERSONNE ! TESTEZ VOS CONNAISSANCES, AFIN DE MESURER VOTRE NIVEAU DE VIGILANCE ET DE DÉCOUVRIR DES CONSEILS ADAPTÉS À VOTRE PROFIL.

■ Vous recevez un appel d'un inconnu qui se prétend conseiller financier et vous propose d'investir dans des produits à haut rendement. Quelle est votre réaction ?

- a) Je raccroche immédiatement.
- b) Je l'écoute, lui pose des questions mais je ne donne aucune information personnelle.
- c) J'accepte qu'il vienne me présenter ses placements très attractifs à mon domicile.

■ Connaissez-vous la spécificité des cryptoactifs comme le Bitcoin ou l'Ethereum ?

- a) Oui, je sais qu'il s'agit d'actifs très spéculatifs et qu'il faut se méfier des acteurs non régulés qui agissent dans ce secteur.
- b) Je sais seulement que ce sont des placements très risqués.
- c) Non, je n'en ai jamais entendu parler.

■ Vous avez reçu un SMS de l'assurance maladie qui vous demande de cliquer sur un lien pour conserver votre Carte Vitale. Que faites-vous ?

- a) Je ne clique jamais sur des liens reçus par SMS ou e-mail sans avoir contacté au préalable l'expéditeur.
- b) Après un temps de réflexion, je finis par ne pas cliquer sur le lien.
- c) Pas question de perdre ma Carte Vitale, je clique immédiatement sur le lien.



■ Dans une foire, un vendeur vous propose un matelas avec une remise de 20 %. Que faites-vous ?

- a) Je prends le temps de me renseigner par moi-même sur le sérieux de l'entreprise.
- b) Je le commande car je pense pouvoir bénéficier d'un délai de rétractation.
- c) Je l'achète et paie immédiatement, pas question de laisser passer une bonne affaire.

Avec un tel rendement, je vais pouvoir m'offrir cette fameuse croisière l'été prochain !



■ Un agent EDF sonne à votre porte pour contrôler votre compteur qui aurait un problème. Quelle est votre attitude ?

- a) J'appelle le service client EDF pour m'assurer de la réalité de la situation, avant de le laisser entrer.
- b) Je lui demande de voir sa carte professionnelle, avant de le laisser entrer.
- c) Je le laisse entrer pour lui permettre d'effectuer au plus vite la réparation.

■ Vous recevez un e-mail d'un ami bloqué à l'étranger qui vous demande en urgence de lui envoyer de l'argent. Que faites-vous ?

- a) Je supprime l'e-mail et j'appelle mon ami pour l'informer que son compte de messagerie a été piraté.
- b) Je contacte mon ami directement par téléphone pour vérifier sa situation avant d'agir.
- c) Je transfère immédiatement de l'argent à mon ami pour l'aider au plus vite.

Quel est votre profil ?

Commencez par calculer votre score total à l'aide de ce barème :
A) 3 POINTS B) 2 POINTS C) 0 POINT



DE 16 À 18 POINTS : L'EXPERT AVERTI

Bravo, vous êtes extrêmement prudent et vous ne faites pas confiance au premier venu. Qu'elles soient classiques ou numériques, vous êtes bien informé sur les arnaques qui circulent. Vous savez rester calme et gérer vos émotions. Ce qui vous permet d'adopter les bons réflexes. **Continuez à être vigilant et à vous tenir régulièrement informé des derniers pièges qui circulent.**



DE 10 À 15 POINTS : LE MÉFIANT PERFECTIBLE

Vous êtes prudent, mais pas encore suffisamment. Vous avez connaissance de nombreuses arnaques mais certaines de vos informations nécessitent d'être précisées et mises à jour. En particulier, celles circulant sur Internet qui évoluent rapidement. Vous savez adopter de bons gestes, mais certains sont encore insuffisants. **Soyez particulièrement vigilant notamment dans les situations qui jouent sur l'urgence ou la peur afin d'obtenir une réaction impulsive de votre part.**



DE 0 À 9 POINTS : LE PROFIL À RISQUE

Vous êtes la victime idéale pour les démarcheurs malhonnêtes et les cybercriminels. Bien que vous ne soyez pas particulièrement intéressé par le sujet, **il est essentiel aujourd'hui de vous informer et de savoir quels comportements adopter face à des scénarios classiques. Parlez-en peut-être à un proche** afin qu'il vous explique quelques gestes simples à adopter. N'hésitez pas non plus à consulter des sites spécialisés fiables tels que www.mesquestionsdargent.fr ou www.cybermalveillance.gouv.fr.



ADRESSES UTILES

www.mesquestionsdargent.fr

www.cybermalveillance.gouv.fr



« On m'a dit que les **arnaqueurs utilisaient la psychologie**, que cela signifie-t-il concrètement ? »

PEUR, CURIOSITÉ, ENVIE, GÉNÉROSITÉ, CULPABILITÉ... LES ARNAQUES FINANCIÈRES REPOSENT TOUJOURS SUR LES MÊMES RESSORTS PSYCHOLOGIQUES ET AFFECTIFS. LES ESCROCS EXPLOITENT NOS ÉMOTIONS AFIN DE MIEUX TROMPER NOTRE CONFIANCE.

Autrefois, le faux policier sonnant à la porte, l'artisan malhonnête invoquant de prétendus travaux urgents ou encore les matelas de piètre qualité vendus à des prix exorbitants sur les marchés ou les foires... Aujourd'hui, bien que les méthodes aient évolué, les escrocs n'ont pas changé

fondamentalement de stratégie. Ils manipulent toujours nos émotions, mais de manière beaucoup plus ciblée. Les recours à la peur ou à l'urgence restent particulièrement efficaces. **Ils exploitent aussi la confiance en se présentant comme des professionnels**

compétents, en utilisant des logos ou des noms reconnus et un langage technique. Ce mécanisme éprouvé conduit leurs futures victimes à être moins méfiantes face à des interlocuteurs qui semblent apparemment compétents et donc fiables. Un autre stratagème consiste à jouer sur l'illusion d'une offre exclusive à ne surtout pas rater car réservée à « quelques privilégiés ». L'usurpation d'identité d'organismes officiels (banque, assurance maladie, impôts...) rend les

messages et les demandes plus crédibles... et donc plus difficiles à repérer. Les seniors, confrontés depuis longtemps aux arnaques classiques, bénéficient toutefois d'une expérience précieuse pour mieux déjouer les nouveaux pièges en ligne. Enfin, **les cybercriminels s'adaptent en permanence à l'actualité** pour rendre leurs méthodes plus convaincantes. Par exemple, en périodes de fêtes, les SMS frauduleux concernant l'envoi de colis bloqués, ou l'été, de fausses annonces sur des plateformes bien

connues de location. Personne n'est à l'abri de telles manipulations psychologiques, quel que soit son âge ou son profil. **Il est donc**

essentiel de comprendre ces mécanismes pour mieux reconnaître les tentatives de fraudes et pour s'en protéger efficacement. ■



RENCONTRE

3 questions à

NATHALIE GRANIER,
PSYCHOLOGUE SPÉCIALISÉE
EN CYBERCRIMINALITÉ

1 Comment les cybercriminels font-ils pour jouer avec nos émotions ?

Les cybercriminels ne sont pas seulement des techniciens experts dans le piratage de nos ordinateurs et téléphones. Ils ont, en outre, **acquis une maîtrise impressionnante des mécanismes psychologiques.**

Ils savent utiliser avec beaucoup d'habileté nos émotions, comme la peur ou la curiosité, afin de déclencher un comportement impulsif, difficile à contrôler. **Leur but est de nous inciter à agir de manière précipitée**, sans prendre le temps de réfléchir, exploitant ainsi notre instinct plutôt que notre raison.



Crédit photo : ANOZIR WAY

“Les cybercriminels (...) savent déclencher un comportement impulsif, difficile à contrôler.”

2 Comment font-ils pour personnaliser leurs attaques ?

Les cybercriminels vont utiliser les informations personnelles déjà disponibles en ligne **comme nos coordonnées, nos habitudes d'achat grâce aux traces que nous laissons, les photos ou les avis** que nous publions sur Internet et les réseaux sociaux. Ils peuvent aussi acheter des fichiers commerciaux. Ces données ainsi récoltées leur permettent de dresser un profil détaillé de leur victime et de personnaliser leurs e-mails

ou SMS. Ces messages personnalisés se révèlent dix fois plus efficaces que des messages collectifs et impersonnels.

3 Que faire pour ne plus en être victime et gérer ses émotions au bon moment ?

Si l'on a déjà été victime d'un cybercriminel, il ne faut pas hésiter à

en parler autour de soi. Il s'agit d'une expérience traumatisante, un véritable choc psychologique. Devant un e-mail, un SMS ou un appel apparemment urgent, **il est essentiel de ne jamais agir dans la précipitation.** Il faut savoir garder son calme afin de prendre le temps d'analyser la réalité de la situation.

« Y a-t-il toujours les traditionnelles arnaques au démarchage à domicile ? »

« Que dois-je faire si une personne me demande de vérifier mon compteur électrique ? »

Un prétendu agent EDF, un policier ou un réparateur sonne à votre porte pour un contrôle ou une réparation dans l'urgence. **Son objectif : pénétrer chez vous** pour vous dérober des objets de valeur, de l'argent liquide et/ou exécuter des travaux inutiles facturés à des prix exorbitants.

QUE FAIRE SI J'AI ÉTÉ PIÉGÉ ?

Déposez plainte. Déclarez les objets volés à votre assurance multirisque habitation. Si vous vous apercevez que votre chéquier a été volé, contactez immédiatement votre banque pour faire opposition.

COMMENT JE FAIS POUR L'ÉVITER ?

Ne laissez entrer personne chez vous, sous aucun prétexte, sans vérifier au préalable son identité. Appelez l'organisme, ou l'entreprise, censé être représenté. Le temps de l'appel, refermez votre porte et laissez le professionnel patienter à l'extérieur. Au moindre doute, refusez l'accès à votre domicile et alertez les autorités locales (mairie, police municipale...).

« J'ai entendu parler d'une arnaque au matelas, en quoi cela consiste-t-il exactement ? »

Sur les marchés, les parkings de supermarché ou dans les foires, des vendeurs vous proposent des matelas à un prix imbattable. Ils précisent que le paiement s'effectuera à la livraison. Le jour du rendez-vous, la somme réclamée peut atteindre plusieurs milliers d'euros. Pris au dépourvu, et sous la pression des malfaiteurs, les victimes finissent par céder et payer des sommes exorbitantes. Des variantes de ce type d'arnaques existent : les arnaqueurs peuvent également vous démarcher directement par téléphone ou à votre domicile.

Heureusement, il y a des solutions !

BIEN QU'ANCIENNES, ELLES N'ONT RIEN PERDU DE LEUR EFFICACITÉ. EN ADOPTANT CERTAINS BONS RÉFLEXES, IL EST POSSIBLE DE LES DÉJOUER ET D'EN LIMITER LES CONSÉQUENCES.

QUE FAIRE SI J'AI ÉTÉ PIÉGÉ ?

Si vous n'avez signé qu'un bon de commande, faites jouer le délai légal de rétractation de 14 jours en adressant au vendeur une demande d'annulation par lettre recommandée avec accusé de réception. Alertez la Direction départementale de la protection des populations (www.economie.gouv.fr/dgccrf/annuaire-des-services-deconcentres), et les organisateurs si la vente a eu lieu sur un marché ou une foire. Déposez plainte. Conservez le maximum de preuves (publicité, bon de commande, facture, SMS...).

COMMENT JE FAIS POUR L'ÉVITER ?

En cas de démarchage, ne faites entrer personne chez vous et déclinez toutes propositions. Ne répondez jamais aux sollicitations par téléphone, courriers ou autres vous invitant à vous rendre à un stand éphémère. Préférez les circuits classiques de magasins de literies ou d'ameublement.

« Un chèque que je n'ai jamais fait a été débité de mon compte, que puis-je faire ? »

Bien que de moins en moins utilisé dans la vie quotidienne, le chèque continue à intéresser les escrocs. **Leurs méthodes vont du vol de chèques (ou de chéquiers) vierges à votre insu à la falsification de chèques**, consistant à modifier le nom du bénéficiaire, le montant indiqué ou la ligne magnétique (zone de chiffres en bas).

QUE FAIRE SI J'AI ÉTÉ PIÉGÉ ?

Si le chèque a été volé, falsifié ou encaissé frauduleusement, faites immédiatement opposition auprès de votre banque. Si aucune faute ou négligence ne peut vous être reprochée, la banque est tenue de bloquer le paiement en cas d'opposition (article L. 131-35 du code monétaire et financier). Déposez plainte.

COMMENT JE FAIS POUR L'ÉVITER ?

Remplissez vos chèques à l'encre noire, en tirant des traits pour ne laisser aucun espace utilisable. Ne laissez jamais votre carnet de chèques sans surveillance et vérifiez régulièrement vos relevés bancaires. Soyez attentifs si vous attendez la remise d'un chéquier par La Poste : la plupart des fraudes sont consécutives à un vol de chéquier pendant sa livraison. Lorsque c'est possible, allez chercher votre chéquier en agence ou privilégiez d'autres moyens de paiement davantage sécurisés, comme les virements bancaires.



ADRESSES UTILES

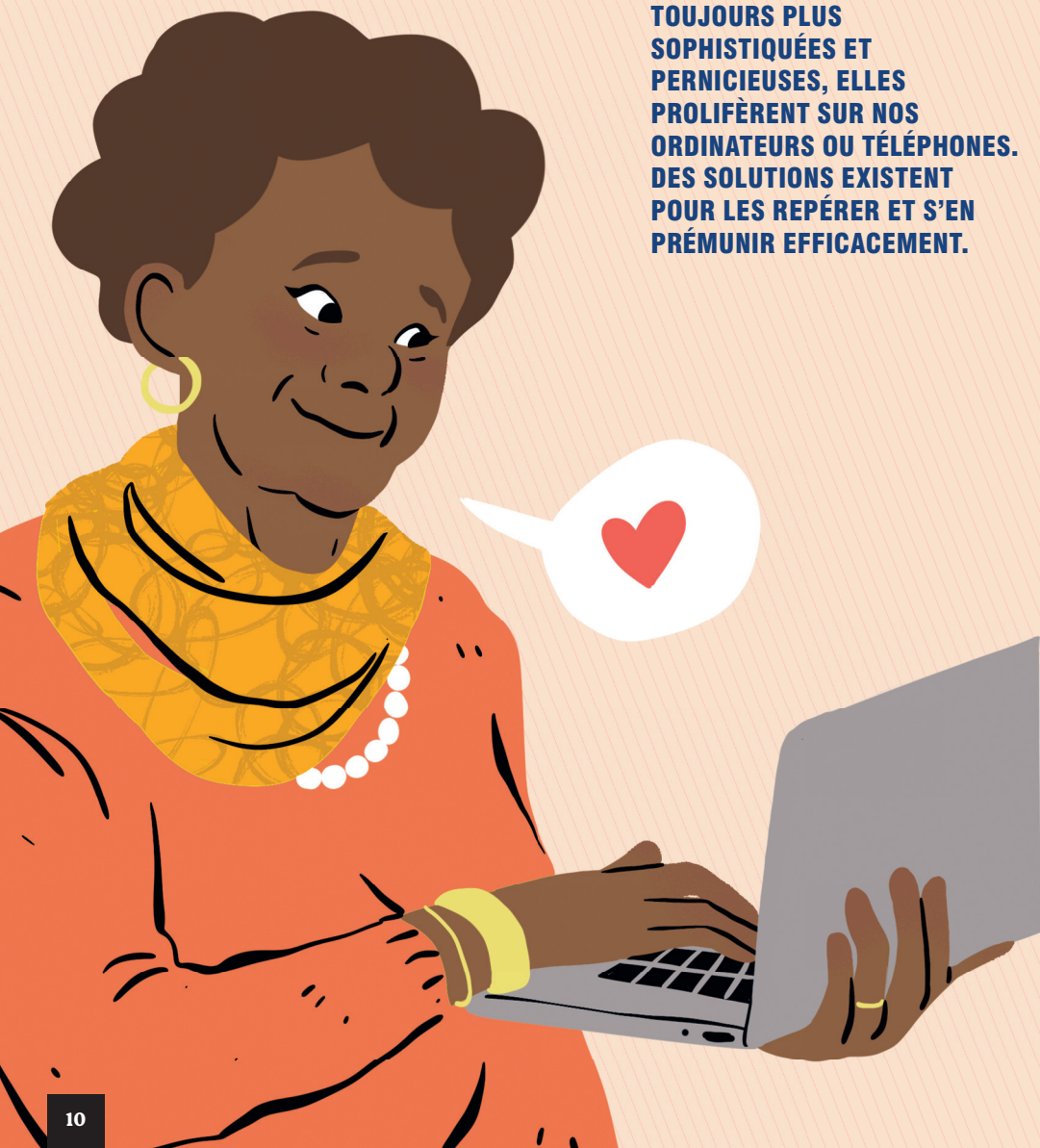
Pour signaler un problème avec une entreprise : <https://signal.conso.gouv.fr>

Pour un accompagnement et des conseils en cas de vol ou d'escroquerie : France Victimes tél. 116 006 (appel gratuit) ou victimes@france-victimes.fr



« Quelles sont les nouvelles arnaques sur **Internet** ou par **SMS** ? »

TOUJOURS PLUS SOPHISTIQUÉES ET PERNICIEUSES, ELLES PROLIFÈRENT SUR NOS ORDINATEURS OU TÉLÉPHONES. DES SOLUTIONS EXISTENT POUR LES REPÉRER ET S'EN PRÉMUNIR EFFICACEMENT.



« On me dit de me méfier de certains e-mails et SMS frauduleux, mais comment les reconnaître ? »

Vous recevez un message prétendument envoyé par un organisme officiel (les impôts, l'assurance maladie...), un créancier ou une société de livraison. Ce message vous incite à cliquer sur un lien sous prétexte de régler une urgence : payer une amende, réactiver votre Carte Vitale, reprogrammer un rendez-vous avec un livreur... En cliquant vous serez redirigé vers un site Internet frauduleux où il vous sera demandé de fournir des informations personnelles et/ou vos coordonnées bancaires.

QUE FAIRE SI J'AI ÉTÉ PIÉGÉ ?

Si votre carte bancaire est utilisée à votre insu, contactez sans tarder votre banque pour faire opposition. Si vous avez été débité frauduleusement, la banque vous remboursera à condition que vous n'ayez pas fait preuve de négligence grave (article L. 133-18 du code monétaire et financier). C'est à la banque de le prouver. Déposez plainte.

COMMENT JE FAIS POUR L'ÉVITER ?

Ne cliquez jamais sur un lien internet dans un SMS ou un e-mail non sollicité. N'appellez jamais les numéros de téléphone qui y sont mentionnés. Supprimez immédiatement ce genre de messages.

« Est-il sérieux de trouver un sac neuf d'une grande marque pour 10 € ? »

Un produit à un prix anormalement bas sur un site inconnu ou, au contraire, sur un site qui semble être celui d'une marque réputée doit vous alerter. Une fois votre paiement effectué, vous ne recevrez jamais votre commande.

QUE FAIRE SI J'AI ÉTÉ PIÉGÉ ?

Contactez immédiatement votre banque pour faire opposition à votre carte bancaire. Déposez plainte.

COMMENT JE FAIS POUR L'ÉVITER ?

Recherchez dans les onglets « Mentions légales » ou « Conditions générales de vente » les coordonnées de l'entreprise puis vérifiez si elle existe bien sur www.societe.com. S'agissant d'un site d'une marque connue, lisez minutieusement l'adresse url afin de vérifier si elle ne comporte pas une modification ou une inversion volontaire de lettres pour vous induire en erreur.

« Comment reconnaître les appels frauduleux provenant d'une usurpation d'identité de ma banque ? »

Vous recevez un appel d'un inconnu se présentant comme « conseiller bancaire » ou « agent du service anti-fraude » de votre banque qui prétend avoir identifié des actions suspectes sur votre compte bancaire. Afin de les bloquer, il vous demande les codes que vous avez reçus par SMS ou de valider des actions directement via votre application bancaire. Ces démarches lui permettent de valider à votre insu des opérations frauduleuses (achats, virements, ajouts de nouveaux bénéficiaires...) sur votre compte.

QUE FAIRE SI J'AI ÉTÉ PIÉGÉ ?

Contactez votre banque pour bloquer les transactions frauduleuses. Si un paiement a déjà été validé, demandez son remboursement en fournissant des preuves des circonstances de la fraude. Les banques sont légalement tenues de vous rembourser, sauf fraude ou négligence grave de votre part (article L. 133-18 du code monétaire et financier). À charge pour la banque de le prouver. Dans un rapport du 16 mai 2023, l'Observatoire de la sécurité des moyens de paiement confirme que l'existence d'une authentification ▶

► forte ne suffit pas pour considérer que la transaction a été autorisée. Dans tous les cas, déposez plainte.

COMMENT JE FAIS POUR L'ÉVITER ?

Ayez en tête qu'aucun conseiller ne vous demandera jamais vos codes ou mot de passe par téléphone. Ne validez aucune opération bancaire sur votre smartphone, si vous n'en êtes pas personnellement à l'origine. Au moindre doute, rappelez votre banque au numéro habituel.

« Existe-t-il des investissements à forte rentabilité sans risques ? »

Des livrets à rendements élevés, des opportunités d'investissements dans des chambres d'Ehpad, des parkings, des crypto-actifs... Que vous ayez été démarché ou appelé après avoir visité un site de trading en ligne, de faux conseillers vous manipulent pour mieux vous soutirer de l'argent. Parfois, ils utilisent abusivement le nom et l'image d'acteurs ou de chanteurs qui prétendent vouloir vous aider à faire fructifier votre argent.

« J'ai reçu un appel au secours d'un ami qui me réclame en urgence de l'argent. Que faire ? »

Par SMS, e-mail ou sur les réseaux sociaux, un(e) ami(e) ou un membre de votre famille vous demande de lui envoyer rapidement de l'argent (par virement, Western Union...) pour le dépanner. En fait, le compte de messagerie de votre proche a été piraté et l'appel à l'aide provient d'un cybercriminel.

QUE FAIRE SI J'AI ÉTÉ PIÉGÉ ?

Si vous avez transféré de l'argent, contactez immédiatement votre banque pour tenter de bloquer ou d'annuler le paiement. Déposez plainte. Alerte votre proche pour qu'il modifie ses mots de passe.

COMMENT JE FAIS POUR L'ÉVITER ?

Vérifiez l'identité de l'expéditeur du message en le contactant directement (par e-mail, SMS, téléphone...).

QUE FAIRE SI J'AI ÉTÉ PIÉGÉ ?

Déposez plainte. Conservez tous les documents (e-mails, SMS, publicités, contrats...) reçus ou signés. Signalez l'arnaque en appelant le 34 14, numéro gratuit de la Banque de France.

COMMENT JE FAIS POUR L'ÉVITER ?

Prenez toujours le temps de la réflexion. Fuyez les promesses de rendements anormalement élevés, sûrs et garantis. Ne laissez jamais vos coordonnées personnelles (téléphone,

e-mail, pièces d'identité, RIB, IBAN, justificatifs de domicile...) sur des formulaires en ligne. Si l'interlocuteur se fait insistant et vous culpabilise, ne donnez pas suite. Consultez les listes noires de l'AMF (<https://protectepargne.amf-france.org>) et l'ACPR (www.abefinfoservice.fr) qui recensent les acteurs non autorisés du secteur, ainsi que les listes blanches de ceux autorisés. Vérifiez que votre interlocuteur figure bien sur www.orias.fr ou www.regafi.fr.

DES PLATEFORMES SPÉCIALISÉES POUR COMBATTRE LA CYBERCRIMINALITÉ



Perceval : le service du ministère de l'Intérieur pour signaler une fraude à la carte bancaire sur service-public.fr/particuliers/vosdroits/R46526



Pharos : pour alerter sur tout contenu illicite sur Internet sur Internet-signalement.gouv.fr



Thésée : pour permettre aux victimes d'e-escroquerie de déposer plainte sur service-public.fr/particuliers/vosdroits/R45758



www.cybermalveillance.gouv.fr

Et donc dans cet e-mail tu disais être coincé aux Galapagos et avoir besoin d'un virement urgent...



« Comment reconnaître un faux RIB ? »

Vous êtes induit en erreur par un e-mail usurpant l'identité d'un créancier (artisan, notaire, bailleur...) avec lequel vous êtes effectivement en relation et vous informant d'un changement de coordonnées bancaires. Vous procédez au virement sur ce nouveau compte qui s'avère frauduleux.

QUE FAIRE SI J'AI ÉTÉ PIÉGÉ ?

Si vous vous en apercevez rapidement, contactez votre banque pour tenter de bloquer ou de rappeler le virement. Déposez plainte.

COMMENT JE FAIS POUR L'ÉVITER ?

Méfiez-vous des demandes urgentes ou inhabituelles de changement de RIB par courriel ou SMS. Téléphonez systématiquement au professionnel afin de vérifier ses coordonnées bancaires.



Credit photo : Booké 2024.

RENCONTRE

3 questions à

FRANCE MAYER,

DIRECTRICE DES RELATIONS AVEC LES ÉPARGNANTS ET DE LEUR PROTECTION DE L'AUTORITÉ DES MARCHÉS FINANCIERS (AMF)

1 Quelles sont les arnaques à l'investissement financier les plus fréquentes ?

En plein essor, ce type d'arnaques touche de plus en plus les particuliers. Selon notre dernière enquête réalisée par BVA Xsight en septembre 2024, 3,2 % des Français en auraient été victimes. Cette proportion a pratiquement triplé en trois ans. **Les réseaux sociaux, véritable caisse de résonance, amplifient le phénomène de la fraude.** Parmi les plus courantes, on recense celles autour des crypto-actifs, des faux placements verts, par exemple ceux dans des parkings équipés de bornes électriques.

2 Quels sont les stratagèmes utilisés par les escrocs ?

Les escrocs se renouvellent et adaptent constamment leurs

modes opératoires, qui deviennent de plus en plus sophistiqués. **Ils utilisent, notamment, la réputation de certains journaux en y insérant de la publicité ou des publi-communiqués sur de fausses offres d'investissement. Ils n'hésitent pas à usurper l'identité de sociétés existantes.** Une de leur dernière technique est de recontacter un épargnant qui s'est déjà fait arnaquer sur un site frauduleux et de lui proposer de l'aider à récupérer son argent en payant à nouveau un certain montant.

3 Comment évaluer rapidement le risque d'un investissement ?

L'AMF met à disposition sur son site, <https://protectepargne.amf-france.org>, un court questionnaire permettant **un diagnostic pour évaluer le niveau de risque d'un investissement et déterminer s'il s'agit d'une potentielle arnaque.**



« Mon ordinateur affiche un message d'alerte indiquant qu'il est infecté par un virus, que dois-je faire ? »

L'écran de votre ordinateur se fige, il vous est demandé d'appeler le numéro d'assistance qui s'affiche. Surtout ne le faites pas, ces prétendus techniciens vous factureront plusieurs centaines d'euros pour un dépannage inexistant. Pire, parfois, ils prendront le contrôle de votre ordinateur pour accéder à vos données personnelles (mots de passe, pièce d'identité...).

QUE FAIRE SI J'AI ÉTÉ PIÉGÉ ?

Fermez la fenêtre d'alerte en appuyant simultanément sur les touches Alt et F4 pour un PC, ou Command et Q sur un Mac. Si le problème persiste, consultez un dépanneur informatique fiable. Sur www.cybermalveillance.gouv.fr, en cliquant sur l'onglet "À propos" puis sur "Les prestataires", vous accédez à une assistance par des professionnels certifiés (service payant).

COMMENT JE FAIS POUR L'ÉVITER ?

Ne naviguez pas sur des sites peu fiables (notamment de téléchargements gratuits de films). Ne cliquez jamais sur les liens d'e-mails suspects.

« Des personnes mal intentionnées sur les sites de rencontre peuvent-elles me faire chanter ? »

Sur des sites de rencontre ou les réseaux sociaux, un escroc se fait passer pour une personne sincère à la recherche d'une relation amoureuse sérieuse. Une fois gagnée votre confiance, il vous demande de l'argent en invoquant des difficultés imprévues : frais médicaux, problèmes administratifs ou judiciaires... Les sommes demandées sont généralement de plus en plus importantes.

QUE FAIRE SI J'AI ÉTÉ PIÉGÉ ?

Bloquez immédiatement la personne sur les réseaux sociaux, les applications de messagerie et sur votre téléphone. Signalez l'escroquerie au site de rencontre et aux réseaux

sociaux concernés. Si vous avez mis en place des virements récurrents, contactez sans tarder votre banque pour qu'elle y mette fin. Déposez plainte. Conservez le maximum de preuves (capture d'écran du profil, numéros de téléphone, messages reçus, avis de virement...).

COMMENT JE FAIS POUR L'ÉVITER ?

Si votre interlocuteur prévoit de vous rencontrer mais que cela n'arrive jamais, cela doit vous alerter. Vérifiez les informations fournies par la personne : une recherche rapide sur l'image du profil ou sur l'histoire de l'individu peut parfois révéler une fraude. Au moindre doute, parlez-en à un proche.

« Où risque-t-on le plus de trouver de faux QR codes ? »

Des QR codes frauduleux sont affichés sur de faux avis de contravention ou de faux avis de passage de La Poste. En les scannant, vous serez redirigé vers un site frauduleux où l'on cherchera à vous faire communiquer des informations personnelles ou à vous convaincre d'effectuer un paiement.

QUE FAIRE SI J'AI ÉTÉ PIÉGÉ ?

Si vous avez fourni des informations personnelles, contactez immédiatement votre banque pour bloquer d'éventuels prélèvements et surveillez vos comptes pour repérer des transactions suspectes.

COMMENT JE FAIS POUR L'ÉVITER ?

Ne scannez pas un QR code dans un lieu public, sans vérifier son origine. Préférez saisir vous-même l'adresse d'un site sur votre appareil. Si un QR code est affiché sur un automate, vérifiez qu'il n'a pas été collé par-dessus l'original.

« Une application pour contrôler mon rythme cardiaque peut-elle vraiment être malveillante ? »

Pour surveiller votre fréquence cardiaque ou activer des équipements connectés comme des caméras, vous êtes invité à télécharger une application gratuite sur votre smartphone. En réalité, l'application exécute des actions à votre insu (appels de numéros surtaxés, abonnements fictifs...) faisant grimper votre facture de téléphone.

QUE FAIRE SI J'AI ÉTÉ PIÉGÉ ?

Désinstallez immédiatement

l'application. Contrôlez vos relevés bancaires et signalez tout débit inconnu à votre banque. Alerte votre opérateur Internet de l'augmentation frauduleuse de votre facture.

COMMENT JE FAIS POUR L'ÉVITER ?

Utilisez uniquement les plateformes reconnues, comme Apple Store (iPhone) ou Google Play Store (Android). Lisez les avis d'utilisateurs. Évitez de télécharger les applications peu connues ou mal notées.

RENCONTRE

2 questions à

JÉRÔME NOTIN,
DIRECTEUR GÉNÉRAL DE LA PLATEFORME
CYBERMALVEILLANCE.GOUV.FR

Crédit photo : Pierre Morel.



1 Quelles sont les missions de la plateforme en ligne ?

Créé en 2017, il s'agit d'un dispositif national d'assistance aux victimes d'actes de cybermalveillance, de sensibilisation aux risques numériques et d'observation de la menace en France. Concrètement, grâce à un diagnostic rapide en ligne, **le site permet d'aider les victimes dans leurs démarches** afin de les orienter vers le téléservice adéquat (Thésée, Pharos,

Perceval...). Il propose également un annuaire des prestataires techniques (réparateurs informatiques, installateurs de logiciels...) formés à la cybersécurité sur tout le territoire afin de réparer ou nettoyer les appareils. **Il suffit de les contacter pour obtenir un devis (gratuit) personnalisé**, avant toute intervention payante. Des fiches pratiques, des vidéos, des tests de connaissance sont également en ligne afin d'informer et de prévenir les cyberarnaques.

2 Quelles sont les évolutions récentes ?

En observant la menace au quotidien, nous avons mis en évidence que les arnaques gagnent en sophistication. C'est pourquoi, la plateforme enrichit en permanence ses **contenus et les outils mis à la disposition du grand public**. Ainsi, depuis décembre 2024, nous avons intégré à la plateforme la possibilité d'échanger directement par tchat avec un policier ou un gendarme.

ADRESSES UTILES

Pour l'assistance aux victimes de cybermalveillance : www.cybermalveillance.gouv.fr



Le site du ministère de l'Intérieur (www.masecurite.interieur.gouv.fr) vous permet notamment d'échanger avec un policier et de prendre un rendez-vous dans un commissariat.



Épargne Info Service : tél. 01 53 45 62 00, la plateforme de l'AMF pour répondre à vos questions sur les produits financiers et les arnaques à l'investissement.



Info-Escroqueries : tél. 0 805 805 817 (appel gratuit).



Quels sont les bons réflexes à adopter sur Internet ?

SI LES ARNAQUES SONT TOUJOURS PLUS PERFECTIONNÉES, BEAUCOUP PEUVENT ÊTRE ÉVITÉES GRÂCE À DES GESTES SIMPLES ET EFFICACES.

1 CHOISISSEZ DES MOTS DE PASSE SOLIDES.

Avec au moins huit signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux (@, &...). **Choisissez un mot de passe différent pour chacun de vos comptes** et changez-en régulièrement.

2 METTEZ À JOUR VOS LOGICIELS, APPLICATIONS ET ANTIVIRUS.

Afin de **corriger les failles de sécurité** dont sont friands les pirates informatiques.

3 ACCEPTEZ LA DOUBLE AUTHENTIFICATION DES SERVICES EN LIGNE.

Pour valider une opération, outre votre mot de passe, une seconde étape, comme l'envoi d'un SMS ou d'un e-mail avec un code, sera exigée.

4 TÉLÉCHARGEZ APPLICATIONS ET FICHIERS UNIQUEMENT SUR DES SITES OFFICIELS.

Préférez Apple Store ou Google Play Store. **Bannissez les sites Internet de téléchargement gratuits** de films et de vidéos qui regorgent souvent de virus.

5 SAUVEGARDEZ RÉGULIÈREMENT VOS DONNÉES.

Faites une copie de vos fichiers et autres documents personnels sur une clé USB, un disque dur externe ou coffre-fort électronique.

7 MÉFIEZ-VOUS TOUJOURS DE MESSAGES INHABITUELS OU PROVENANT D'INCONNUS.

Partez du principe qu'ils sont presque tous frauduleux. Lisez-les calmement et ne réagissez jamais sous le coup de l'émotion.

6 SOYEZ ATTENTIF À CE QUE VOUS PARTAGEZ.

Limitez l'accès à vos comptes sur les réseaux sociaux à vos amis et relations proches. Soyez vigilant sur ce que vous mettez en ligne (photos, avis...).

8 VÉRIFIEZ LA SÉCURITÉ DU SITE AVANT D'EFFECTUER UN PAIEMENT EN LIGNE.

À minima, l'adresse URL du site doit commencer par « **https://** » et être suivie d'un cadenas fermé.

9 NE VOUS FIEZ PAS AU NUMÉRO QUI S'AFFICHE SUR LE TÉLÉPHONE PORTABLE.

Au moindre doute, raccrochez et rappelez votre interlocuteur à un numéro que vous connaissez.

10 À L'EXTÉRIEUR, CONNECTEZ-VOUS UNIQUEMENT À DES WIFI SÉCURISÉS.

Utilisez les réseaux WiFi dans lesquels vous pouvez avoir confiance. Par exemple, celui d'un hôtel ou d'une médiathèque qui vous fournira un mot de passe pour vous connecter.

