Arnaques en ligne

Comment les repérer ?

Que faire ?

Observatoire du Crédit et de l'Endettement

www.enmieux.be

Cofinancé par l'Union européenne

Wallonie

Cette brochure a été réalisée par l'Observatoire du Crédit et de l'Endettement avec l'aimable collaboration de :

- **Mary Ann Borgers**, coordinatrice, Neniu asbl
- **Leen De Cort**, coordinatrice, AB-Reoc
- **Marie-Astrid Dembour**, magistrat, Parquet de Bruxelles
- **Laurence Hilson**, inspectrice, SPF Economie
- **William Matgen**, legal advisor, CEC Belgique
- **Anais-Lyna Oumouadène**, legal counsel, FSMA
- **Chloé Vanheuverswyn**, coordinatrice du service Périmètre, FSMA
- **Charline Gorez**, Marketing & Communication Specialist, Febelfin

TABLE DES MATIERES

10 conseils pour reconnaître et éviter les arnaques

- ☐ **Vérifier si l'offre n'est pas trop avantageuse par rapport à d'autres.**
  Se poser la question si l'offre n'est pas « trop belle pour être vraie ». Si c'est le cas, il s'agit probablement d'une arnaque !

- ☐ **Vérifier l'identité du vendeur/de l'interlocuteur.**
  Vérifier l'adresse postale, l'adresse mail, le numéro d'entreprise, l'url du site internet ou de l'adresse mail. Quelques outils pratiques en page 31.

- ☐ **Vérifier la réputation du vendeur/de l'interlocuteur.**
  Il vaut mieux ne pas se fier aux évaluations visibles directement sur les sites internet des entreprises, mais effectuer des vérifications sur des moteurs de recherche.

- ☐ **Prendre le temps de lire les contrats et les conditions générales des offres y compris les inscriptions en petits caractères.**
  Des informations importantes sur l'engagement y sont bien souvent dissimulées.

- ☐ **Vérifier que les informations sont bien claires et compréhensibles avant de s'engager.**
  Toute entreprise pratiquant la vente de biens ou de services doit clairement s'identifier, présenter les caractéristiques de son offre et expliquer aux consommateurs leur droit de rétractation. Ne pas hésiter à demander des précisions si ces informations ne sont pas suffisamment claires. Pas d'explication supplémentaire ? Il est prudent de mettre fin à la transaction.

- **Ne jamais communiquer ses mots de passe, informations bancaires, code PIN ou réponse de Digipass.**
  Ces informations doivent absolument rester confidentielles. La banque ne les demandera jamais par téléphone ou par email !

- **Privilégier les paiements par carte de crédit, paypal ou à la réception.**
  Ces moyens de paiement garantissent une certaine protection en cas de problème de livraison ou de fraude.

- **Ne pas répondre aux appels inattendus provenant de numéros de téléphone étrangers inconnus.**

- **Contrôler le numéro de compte sur lequel l'interlocuteur demande de verser de l'argent.**
  Se méfier s'il s'agit d'un compte bancaire ouvert dans un pays différent de celui du siège social ou du vendeur. Pour cela, vérifier que le numéro de compte IBAN correspond bien au pays concerné.

- **Ne jamais céder à l'urgence.**
  L'urgence est un prétexte courant utilisé par les fraudeurs pour créer la panique auprès de leurs potentielles victimes. Ils essaient ainsi de les amener à agir plus rapidement et sans réflexion.

Arnaques spécifiques

A Ventes frauduleuses et publicités trompeuses

Pièges aux abonnements

Julie est séduite par des annonces sur les réseaux sociaux ou des pop-ups sur des sites internet proposant de tester, par exemple, un produit cosmétique aux vertus miraculeuses, de recevoir un cashback, de tester un service de streaming gratuitement...
En cliquant sur l'annonce, Julie est redirigée vers un autre site et est invitée à communiquer ses données personnelles et son numéro de carte de crédit.
S'il s'agit d'une annonce pour un produit, Julie reçoit son colis gratuit comme prévu. 14 jours après la livraison de celui-ci, elle reçoit un 2ème colis, cette fois-ci facturé à un montant important ou directement déduit de sa carte de crédit. Ces livraisons se répètent régulièrement jusqu'à l'intervention de Julie.
S'il s'agit d'une annonce pour un service comme du streaming, par exemple, l'offre n'est effective que pour une courte période et, quelques heures après son inscription, Julie est débitée sur sa carte de crédit.

Comment éviter l'arnaque ?

- ☐ **Lire très attentivement les conditions générales (même s'il s'agit d'un échantillon ou d'un cadeau).**
  Les informations relatives à l'abonnement conclu pour bénéficier de l'offre gratuite sont dissimulées dans les conditions générales de vente.
  Astuce pratique : effectuer une recherche par mots-clés en utilisant des termes tels que « abonnement », « prix » ... pour vérifier qu'il ne s'agit effectivement pas d'une offre conditionnée à un abonnement payant.

- ☐ **Vérifier les cases pré-cochées automatiquement avant de valider la commande.**
  La loi stipule que lorsqu'un consommateur souhaite souscrire un service additionnel lors d'une réservation, il doit en faire explicitement la demande. La case correspondant au service additionnel ne peut dès lors pas être cochée par défaut.

- [ ] **Lire attentivement le mail de confirmation de la commande.**
Cette vérification permet de réagir rapidement et de faire appliquer son droit de rétractation en cas de vente abusive.
Attention, il est probable que le mail arrive directement dans les courriers indésirables. Vérifier régulièrement sa boite mail.

- [ ] **Ne pas contacter les entreprises via des numéros de téléphone surtaxés.**
Ces numéros commencent par 0900 ou 070.
Bon à savoir : les entreprises avec lesquelles les consommateurs ont conclu un contrat sont obligées de leur communiquer un numéro de téléphone gratuit.

- [ ] **D'autres conseils ?**
Voir la checklist des bons conseils p.4.

Comment réagir ?

- [ ] **Renvoyer les colis reçus à la société pour ne pas être facturé.**
Attention : cette action est uniquement possible si le consommateur dispose des instructions de retour de colis.

- [ ] **Dénoncer l'arnaque.**
Où ? Au Point de contact du SPF Economie[1] et à Test-achats[2] s'il s'agit d'un litige interne à la Belgique ou au CEC Belgique[3] s'il s'agit d'un litige impliquant une société dont le siège se situe dans un autre pays européen.

1 Site https://pointdecontact.belgique.be/meldpunt/fr/bienvenue
2 Site https://www.test-achats.be/plainte
3 Site https://www.cecbelgique.be/complaint-wizard-page

Télévendeurs frauduleux

Isabelle reçoit un appel commercial lui proposant de bénéficier d'une offre privilégiée, de recevoir un échantillon gratuit, des chèques voyages, des bons de réduction... Le vendeur insiste sur la gratuité de sa proposition auprès d'Isabelle. Isabelle donne ses coordonnées au vendeur pour recevoir l'offre proposée. Elle reçoit à la place un email avec un contrat d'abonnement ou une facture salée.

Comment éviter l'arnaque ?

- ☐ **Consulter la liste des télévendeurs**
  Le SPF Economie et le CEC Belgique ont créé une liste des télévendeurs[4] pour lesquels ils ont reçu des signalements.

- ☐ **D'autres conseils ?**
  Voir la checklist des bons conseils p.4.

4 Site https://economie.fgov.be/fr/themes/protection-des-consommateurs/arnaques-la-consommation/formes-darnaques/telephoniques/liste-des-televendeurs-et

Comment réagir ?

- ☐ **Consulter régulièrement l'historique des transactions des comptes bancaires et cartes de crédit** pour vérifier que des sommes n'ont pas été prélevées sans autorisation. Contacter la banque en cas de doute.
- ☐ **S'inscrire sur la liste « Ne m'appelez plus »**[5] pour ne plus recevoir d'appels commerciaux non sollicités.
- ☐ **SMS surtaxés non sollicités ? Envoyer STOP par SMS au même numéro.**
  Contacter l'opérateur de téléphonie pour bloquer le numéro si la réception des messages continue.
- ☐ **Victime d'une arnaque ? Que faire ?** Voir page 29.

5 Site https://www.dncm.be

Fausses annonces sur des plateformes de vente en ligne

Adrien découvre, sur une plateforme de location de logements de vacances, une annonce pour la maison de ses rêves. Il contacte le vendeur pour connaître les disponibilités et le montant de la location. Au moment de payer, le vendeur invoque un problème technique et propose à Adrien de réaliser la transaction hors de la plateforme via un virement bancaire, par exemple. La transaction se déroule correctement et Adrien reçoit un mail de confirmation de sa réservation semblant provenir de la plateforme. Arrivé en vacances, Adrien constate que le logement qu'il a réservé n'existe pas en réalité. Désemparé, il ne dispose d'aucun recours vis à vis de la plateforme car la transaction a été réalisée en dehors de celle-ci.

Comment fonctionne une plateforme ?

Une plateforme est un site internet sur lequel les consommateurs doivent créer un compte pour pouvoir entrer en contact avec des vendeurs et conclure des contrats. Il peut s'agir, par exemple, de plateformes de vente de vêtements, de biens, de location de logements de vacances... Lors de la validation d'une transaction, le consommateur est invité à payer le montant dû au vendeur via cette plateforme. L'argent est bloqué et n'est réellement versé au vendeur qu'à partir du moment où la plateforme reçoit la validation du bon déroulement de la transaction. Il est plus sécurisant d'effectuer les paiements uniquement via ces plateformes.

Comment éviter l'arnaque ?

- ☐ **Toujours vérifier le fonctionnement des plateformes dans les conditions générales.**
- ☐ **Ne pas effectuer de transactions financières en dehors des plateformes.**
  Le vendeur souhaite réaliser le paiement en dehors de la plateforme ? Il vaut mieux stopper la transaction.
- ☐ **D'autres conseils ?**
  Voir la checklist des bons conseils p.4.

Comment réagir ?

- ☐ **Vérifier le contenu du mail de confirmation de la transaction et l'adresse mail de l'expéditeur.**
  S'agit-il bien de l'adresse mail officielle de la plateforme ? Si cela n'est pas le cas, contacter la plateforme pour leur signaler l'usurpation d'identité.
- ☐ **Prévenir la plateforme de la fraude ou de la tentative de fraude.**
  En cas de fraude avérée, la plateforme ne peut pas rembourser les sommes versées, mais le consommateur peut tenter d'obtenir un geste commercial.
- ☐ **Victime d'une arnaque ? Que faire ?** Voir page 29.

Faux bureaux de recouvrement

Un télévendeur avait contacté Farid pour une offre concernant des chèques voyage il y a quelques mois. Il avait proposé de lui envoyer les informations par mail afin de lui laisser le temps de réfléchir à son offre. Le courriel avait toutefois atterri dans les courriers indésirables de Farid et le vendeur ne l'avait plus contacté par la suite. Le mail mentionnait que faute de réaction de Farid dans un certain délai, il était présumé avoir accepté l'offre. Après un délai assez important (pouvant parfois aller jusqu'à plus d'un an), Farid est contacté par une agence de recouvrement de dettes néerlandaise concernant l'offre de chèques voyage qu'il est supposé avoir acceptée. Le prétendu bureau de recouvrement exerce alors une pression sur Farid pour qu'il paie rapidement ses dettes.

Qu'est ce qu'une mise en demeure ?

Une mise en demeure est l'ultime courrier de rappel de paiement qui est envoyée avant d'introduire une procédure judiciaire. Une mise en demeure contient les informations suivantes :

- L'identité complète du bureau de recouvrement : nom et dénomination, adresse, n° d'entreprise (BCE), n° de TVA et numéro d'inscription auprès du SPF Economie ;
- L'identité complète du créancier d'origine : identité, adresse, n° de téléphone ;
- Une description claire de l'offre qui a donné naissance à la dette ;
- Une description et justification claires des montants réclamés au débiteur (y compris les dommages intérêts et intérêts moratoires réclamés) ;
- La mention légale obligatoire en gras et caractère distinct indiquant « *Cette lettre concerne un recouvrement amiable et non un recouvrement judiciaire (assignation au tribunal ou saisie)* » ;
- Le délai légal minimal (de 15 jours) avant que d'autres mesures ne soient prises ;
- Les coordonnées de l'autorité de surveillance (SPF économie, Chambre nationale des huissiers de justice, Ordre des avocats...).

Comment éviter l'arnaque ?

- ☐ **Vérifier qu'il s'agit d'une mise en demeure pour un contrat effectivement conclu.**
  S'il s'agit d'un contrat inconnu, ignorer la demande.

- ☐ **Vérifier le contenu de la mise en demeure.**
  Ce courrier contient-il les informations légales obligatoires ? Si non, ignorer le courrier.

- ☐ **Vérifier le langage utilisé dans la mise en demeure.**
  Vérifier la grammaire, les contradictions, les traductions... Si le courrier n'est pas écrit dans un français correct, il est plus prudent de l'ignorer.

- ☐ **Vérifier l'identité du bureau de recouvrement :**
  - Vérifier que le bureau de recouvrement n'est pas repris sur la liste grise du SPF Economie[6] (la liste grise reprend les bureaux de recouvrement pour lesquels le SPF Economie a reçu des signalements).
  - Vérifier que le bureau de recouvrement est inscrit[7] auprès du SPF Economie comme personne pouvant exercer une activité de recouvrement de dettes. Attention, les avocats, huissiers et mandataires de justice ne sont pas repris par cette liste.
  - Le mail provient d'un huissier de justice ? Consulter la liste grise de la Chambre nationale des huissiers de justice[8].

- ☐ **D'autres conseils ?**
  Voir la checklist des bons conseils p.4.

6 Site https://economie.fgov.be/fr/themes/protection-des-consommateurs/arnaques-la-consommation/formes-darnaques/telephoniques/liste-des-televendeurs-et
7 Site https://economie.fgov.be/sites/default/files/Files/Publications/files/Liste-recouvreurs-de-dettes.pdf
8 https://www.huissiersdejustice.be/lhuissier-de-justice/informations-pratiques/fraude-internet

Comment réagir ?

- ☐ **Suspicion d'usurpation d'identité d'une société ?** Contacter l'agence de recouvrement, l'huissier ou l'avocat dont le nom est mentionné sur la mise en demeure via les coordonnées officielles trouvées sur le site de la Banque Carrefour Entreprise[9] ou sur le site officiel de l'entreprise.

- ☐ **Contester formellement la dette invoquée** Contester par écrit et de préférence avec un accusé de réception. Le SPF Economie propose un modèle de lettre[10].

- ☐ **Victime d'une arnaque ? Que faire ?** Voir page 29.

9 Site https://economie.fgov.be/fr/themes/entreprises/banque-carrefour-des
10 Site https://economie.fgov.be/sites/default/files/Files/Forms/Empowerment/lettre-type-contester-mise-en-demeure-incasso.docx

Fraude aux investissements

Philippe découvre une annonce pour Investissur proposant des investissements avec de très hauts rendements recommandés par des célébrités. Intéressé, Philippe souhaite en savoir davantage et visite le site internet d'Investissur. Il y complète un formulaire et est ensuite contacté par téléphone. La prise de contact se déroule parfaitement, le discours d'Investissur est clair et Philippe reçoit des réponses précises à ses questions. Il décide alors d'investir une petite somme d'argent. Peu après, il constate l'évolution de son rendement et reçoit une partie de ses gains. Par la suite, Philippe, confiant, est invité à augmenter le montant de ses investissements. Cependant, une fois les sommes d'argent supplémentaires versées, Investissur ferme. Philippe n'a plus de contact avec la société et peut dire adieu à son argent.

Comment éviter l'arnaque ?

- **Examiner les publicités pour des propositions d'investissements** publiées sur les réseaux sociaux, par exemple.
  Se poser la question si elles ne sont pas trop belles pour être vraies.

- **Vérifier l'identité de l'interlocuteur**
  Son nom, l'adresse du siège social et le pays d'établissement sont-ils décrits ? N'accepter une offre que si l'entreprise est clairement identifiable.
  Se méfier des « cloned firm ». Il est fréquent que les escrocs usurpent l'identité de sociétés autorisées. L'examen des adresses électroniques ou des données de contact des sociétés en question permet de détecter ce type de fraude.
  Suspicion d'usurpation d'identité ? Prévenir la société usurpée via les coordonnées officielles trouvées sur le site de la Banque Carrefour Entreprise[11] ou sur le site officiel de l'entreprise.

- **Vérifier que l'entreprise a un agrément ou est enregistrée officiellement.**
  Pour pouvoir offrir des services et produits financiers en Belgique, les entreprises doivent disposer de l'agrément ou l'enregistrement nécessaire. Il est possible de vérifier ceci sur le site web de la FSMA[12].

- **Vérifier que l'offre est fiable.**
  Faire le test « Suis-je victime d'une arnaque ? » proposé sur le site de la FSMA[13].

- **Des doutes au sujet d'une offre de services financiers ?**
  Prendre contact avec la FSMA via le formulaire de contact pour les consommateurs[14].

- **D'autres conseils ?**
  Voir la checklist des bons conseils p.4.

11 Site https://economie.fgov.be/fr/themes/entreprises/banque-carrefour-des
12 Site https://www.fsma.be/fr/preteurs
13 Site https://www.fsma.be/fr/attention-aux-fraudes
14 Site https://www.fsma.be/fr/formulaire-de-contact-consommateurs

Comment réagir ?

- ☐ **Ne pas céder aux menaces.**
- ☐ **Couper le contact.**
  Stopper immédiatement tout contact avec les escrocs et arrêter toute transaction financière avec eux (même si la firme réclame un versement complémentaire ou le paiement d'une taxe afin de pouvoir toucher un bénéfice).
- ☐ **Rester vigilant face à de nouvelles tentatives de fraude.**
  Les escrocs n'ont pas de scrupules à contacter les victimes en affirmant vouloir les aider à récupérer leur investissement, une arnaque appelée « recovery room ».
- ☐ **Victime d'une arnaque ? Que faire ?** Voir page 29.

Fraude aux crédits

Véronique connaît actuellement quelques difficultés financières suite à la perte de son emploi. Elle aimerait contracter un crédit pour réaliser des travaux de réparation à son domicile mais les banques refusent. Elle voit une annonce pour un prêt aux conditions très intéressantes sur les réseaux sociaux et contacte le prêteur. Afin de pouvoir bénéficier du crédit, Véronique est invitée à payer des frais (par exemple, des taxes, une prime d'assurance, des frais de dossier...). Une fois ces frais payés, Véronique ne reçoit pas son prêt et n'a plus de contact avec le soi-disant prêteur.

Comment éviter l'arnaque ?

- **Analyser les offres de crédits.**
  Surtout celles proposées sur internet ou au travers des médias sociaux.

- **Vérifier que l'interlocuteur possède l'autorisation** nécessaire pour proposer des offres de crédits via le site de la FSMA[15].

- **Vérifier si l'offre n'est pas trop avantageuse par rapport à d'autres.**
  Une proposition de crédit à des conditions particulièrement avantageuses (montant très élevé au regard de la situation financière du consommateur, taux d'intérêt extrêmement faible, durée de remboursement exceptionnellement longue, etc.) alors que d'autres prêteurs agréés n'accordent généralement pas de tels crédits ? Se poser la question si l'offre n'est pas « trop belle pour être vraie ». Si c'est le cas, il s'agit probablement d'une arnaque !

- **Vérifier l'identité de l'interlocuteur**
  Son nom, l'adresse du siège social et le pays d'établissement sont-ils décrits ? N'accepter une offre que si l'entreprise est clairement identifiable.

15 Site https://www.fsma.be/fr/preteurs

Se méfier des « cloned firm ». Il est fréquent que les escrocs usurpent l'identité de sociétés autorisées. L'examen des adresses électroniques ou des données de contact des sociétés en question permet de détecter ce type de fraude.
Suspicion d'usurpation d'identité ? Prévenir la société usurpée via les coordonnées officielles trouvées sur le site de la Banque Carrefour Entreprise[16] ou sur le site officiel de l'entreprise.

- ☐ **Vérifier que l'offre est fiable.**
  Faire le test « Suis-je victime d'une arnaque ? » proposé sur le site de la FSMA[17].

- ☐ **Des doutes au sujet d'une offre de services financiers ?**
  Prendre contact avec la FSMA via le formulaire de contact pour les consommateurs[18].

- ☐ **D'autres conseils ?**
  Voir la checklist des bons conseils p.4.

16 Site https://economie.fgov.be/fr/themes/entreprises/banque-carrefour-des
17 Site https://www.fsma.be/fr/attention-aux-fraudes
18 Site https://www.fsma.be/fr/formulaire-de-contact-consommateurs

Comment réagir ?

- ☐ **Couper le contact.**
  Stopper immédiatement tout contact avec les escrocs et arrêter toute transaction financière avec eux (même si la firme réclame un versement complémentaire).

- ☐ **Contacter la FSMA.**
  Via le formulaire de contact pour les consommateurs[19] pour introduire une plainte.

- ☐ **Victime d'une arnaque ? Que faire ?** Voir page 29.

19 Site https://www.fsma.be/fr/formulaire-de-contact-consommateurs

D

Fraudes à la banque en ligne

Phishing/smishing

Aida reçoit un mail provenant de sa banque disant que son compte bancaire est bloqué. Elle doit cliquer sur un lien pour en savoir davantage ou pour effectuer l'action demandée. Le lien conduit sur un site internet qui ressemble à un véritable site de banque en ligne. Aida est invitée à introduire ses données personnelles et ses coordonnées bancaires. Les fraudeurs ont alors toutes les informations nécessaires pour vider le compte bancaire d'Aida.

Ce type d'arnaque existe également sous la forme d'un SMS reçu au nom, par exemple, de la banque, d'itsme ou d'une administration. Ce type de phishing est appelé du « smishing ».
Le phishing peut aussi se faire par téléphone.
Les fraudeurs essaient de se faire passer pour des organismes de confiance.

Comment éviter l'arnaque ?

☐ **Vérifier le mail ou le sms reçu :**

- L'adresse mail correspond-t-elle exactement à l'organisation mentionnée ?
- Le mail/sms est-il adressé personnellement ou s'agit-il d'un mail/sms envoyé en masse ?
- Y a-t-il une forme de pression exercée dans la communication ?

☐ **Vérifier le lien du site internet avant de cliquer dessus.**
Comment ? Placer le curseur de la souris sur le lien afin de vérifier l'adresse url exacte du site. L'adresse du site internet semble suspecte ? Ne pas cliquer et supprimer le mail/sms.

- [ ] **Toujours réaliser ses opérations bancaires à partir de son application bancaire habituelle ou aller directement sur le site internet de sa banque.**
  Ne jamais faire de transactions bancaires via un lien reçu dans un message, même si le site ressemble à celui d'une banque !

- [ ] **Ne jamais communiquer des informations personnelles ou bancaires.**
  Ces informations doivent absolument rester confidentielles et ne doivent pas être communiquées en réponse à un mail, un appel téléphonique, un sms, un message sur les réseaux sociaux...

- [ ] **Ne jamais communiquer son code PIN.**
  Ni les réponses du lecteur de carte bancaire et cela même si l'interlocuteur prétend être un banquier.

- [ ] **Ne jamais télécharger de logiciels, d'applications... à partir d'un lien reçu dans un message.**
  Ceux-ci peuvent contenir un virus qui peut accéder à vos données personnelles.

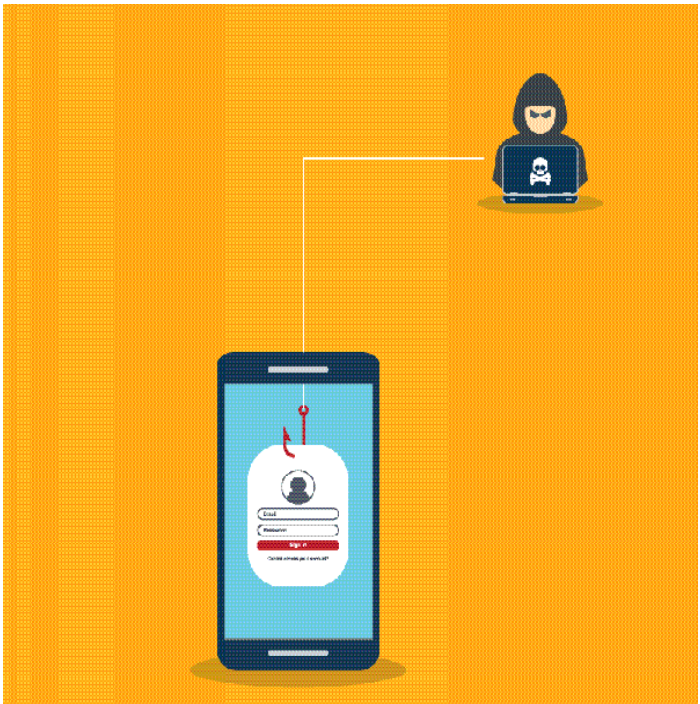
- [ ] **D'autres conseils ?**
  Voir la checklist des bons conseils p.4.

Comment réagir ?

- **En cas de doute :**
  - Stopper toute transaction ;
  - Contacter sa banque pour expliquer la tentative de fraude.

- **Signaler les messages suspects.**
  - Via l'adresse suspect@safeonweb.be. Cela permet d'éviter que d'autres personnes ne tombent dans le piège et supprimer le mail par la suite.
  - Si le message suspect est au nom d'une banque, informer la banque en question. Chaque banque a une adresse mail spécifique dédiée au phishing.

- **Victime d'une arnaque ? Que faire ?** Voir page 29.



Mule financière

Steve (18 ans) est contacté sur les réseaux sociaux par Jonathan. Celui-ci lui propose de gagner de l'argent facilement en échange de l'utilisation de son compte et de sa carte bancaire. Steve accepte, prête sa carte bancaire et donne son code PIN à Jonathan. Jonathan utilise alors le compte bancaire de Steve pour recevoir différentes sommes d'argent, principalement dérobées via du phishing, par exemple. Il en profite également pour vider intégralement le compte de Steve et disparaît par la suite.
Quand les victimes du phishing déposent plainte à la police, elles communiquent le numéro de compte bancaire sur lequel leur argent a été transféré. Jonathan ayant utilisé le compte de Steve, celui-ci est tenu responsable et poursuivi par la justice car, en servant de mule financière, il a fait du blanchiment d'argent. Jonathan a, quant à lui, effacé toute trace de lui-même et reste anonyme.

Comment éviter l'arnaque ?

- **Vérifier si l'offre n'est pas trop belle pour être vraie.**
  Un recruteur approche ses victimes en ligne ou dans la vraie vie et leur propose de l'argent en échange de leur compte bancaire et/ou de leur carte bancaire. N'est-ce pas trop facile ?

- **S'interroger sur la légalité de l'offre.**
  Cette pratique est souvent décrite comme légale, un service entre amis etc. Qu'en est-il réellement ?

Comment réagir ?

- **Ne jamais prêter sa carte de banque ni son compte bancaire !**

- **En cas de doute :**
  - Cesser tout transfert d'argent;
  - Ne pas retirer en cash l'argent qui a été versé sur le compte;
  - Contacter au plus vite la banque ;
  - Faire bloquer la carte bancaire via Card Stop ;
  - Déposer plainte auprès de la police.

E

Fraudes à l'émotion

Fraude à l'amitié et aux sentiments

Emilia, la cinquantaine, vient de divorcer. Elle se sent seule et comble sa solitude en fréquentant les réseaux sociaux. Elle reçoit une demande d'ami d'Esteban avec qui elle se découvre très rapidement de nombreux points communs. Ils communiquent au quotidien sur leurs joies et leurs peines et Emilia trouve en Esteban une oreille compréhensive et attentive. Un lien fort se crée entre eux malgré le fait qu'ils habitent à plusieurs centaines de kilomètres l'un de l'autre. Soudainement, Esteban devient injoignable. Emilia s'inquiète car ce n'est pas dans ses habitudes. Peut-être lui est-il arrivé quelque chose. À sa reprise de contact, Esteban justifie son absence par une problème nécessitant de trouver rapidement une importante somme d'argent. Emilia, mise en confiance, commence à lui envoyer de l'argent pour l'aider à sortir de cette mauvaise passe. Les demandes d'argent vont se répéter et Esteban va se montrer de plus en plus insistant jusqu'à ce qu'Emilia décide de stopper les envois d'argent. Ensuite, Esteban disparaît et Emilia perd la personne qu'elle aimait ainsi que son argent.

Comment éviter l'arnaque ?

- **Vérifier le profil de l'interlocuteur sur les réseaux sociaux.** S'agit-il d'un profil récent ? A-t-il publié plusieurs photos sur le réseau social ? Habite-t-il dans la même région ? A-t-il plusieurs amis sur le réseau social ? Existe-t-il des amis en commun ? S'il s'agit d'une personnalité connue (un chanteur, un comédien...), utilise-t-il un compte certifié ? En cas de doute, refuser les demandes de discussion ou demandes d'amitié.

- **Contrôler la photo de profil de l'interlocuteur en effectuant une recherche.**
Enregistrer la photo et l'importer sur Google images[20] pour voir si l'image n'est pas déjà utilisée par d'autres profils.

20 Site : https://www.google.fr/imghp

Toutefois, depuis mai 2018 et les directives de la protection de la vie privée, il devient de plus en plus difficile de retrouver des photos utilisées qui ne sont pas celles de personnalités connues.

- **Vérifier l'existence réelle de la personne.**
  Lui demander de pouvoir la joindre par téléphone ou en vidéo. La personne ressemble-t-elle à ses photos ? Lors du contact en vidéo, demander à son interlocuteur de se gratter le nez, de faire un geste précis de la main, par exemple, afin de vérifier qu'il ne s'agit pas d'une vidéo pré-enregistrée.

- **Vérifier que l'interlocuteur n'a pas envoyé le même message à d'autres personnes.**
  Effectuer une recherche en tapant le nom de la personne sur les réseaux sociaux ou les groupes de discussion par lequel il est entré en contact.

- **Rester vigilant et garder la tête froide !**
  L'arnaqueur va souvent précipiter la relation : marques d'affection trop rapides, envois de cadeaux ... Garder un esprit critique par rapport au problème de l'interlocuteur et l'excuse donnée.

- **Contrôler l'adresse email de l'interlocuteur.**
  Vérifier qu'elle ne se trouve pas sur la liste mails d'escrocs publiée par l'asbl Neniu[21].

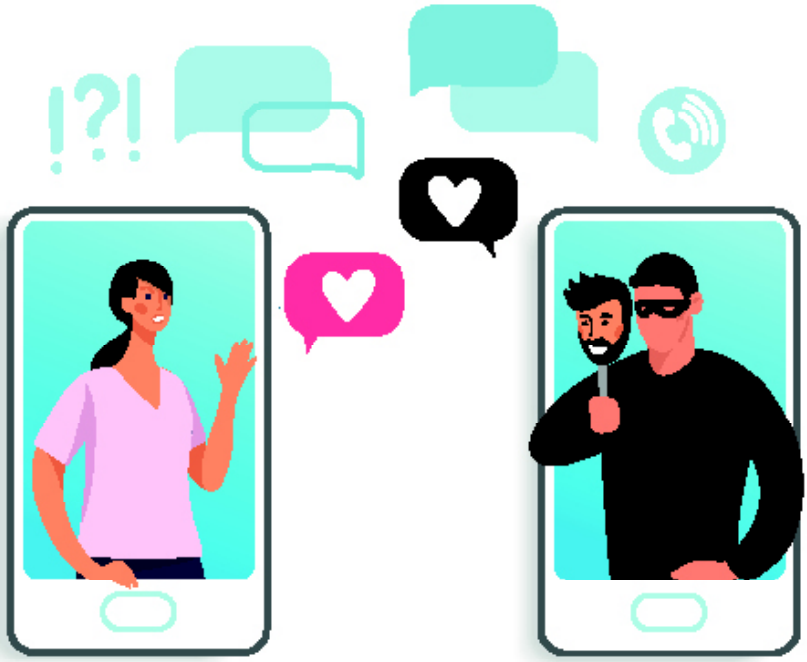
- **Sécuriser ses comptes sur les réseaux sociaux.**
  Vérifier les paramètres de partage d'informations et ne pas partager ses données publiquement. Attention : les informations et photos publiées aident les arnaqueurs à cibler leurs victimes et peuvent même être volées pour être utilisées sur de faux comptes.

- **D'autres conseils ?**
  Voir la checklist des bons conseils p.4.

21 Site https://neniu-assos.org

Comment réagir ?

- **Stopper tout contact avec l'arnaqueur.**
- **Carte d'identité ou passeport perdu ou volé ?** Contacter le service Docstop au 0800/2123.2123 pour éviter le risque d'usage frauduleux des documents et d'éventuelles conséquences financières (ex : ouverture en votre nom d'un abonnement téléphonique, achat par correspondance...).
- **Victime d'une arnaque ? Que faire ?** Voir page 29.



Victime d'une arnaque ? Que faire ?

1 Appeler Card Stop au 078/170.170

Numéro de téléphone à composer pour bloquer immédiatement tous moyens de paiement (cartes, applications ou objets connectés). Card Stop s'occupe également du remplacement de la carte bancaire.
Service disponible 24h/24 et 7j/7.
Card Stop peut également bloquer les applications Payconiq, Apple Pay et Google Pay.
Pour bloquer l'application bancaire ou le compte bancaire, il faut contacter sa banque.

2 Contacter sa banque

En cas de soupçon de fraude ou d'arnaque, contacter immédiatement sa banque. Toutes les données de contact des banques sont disponibles sur le site de Card Stop[22].

3 Remplir un formulaire de contestation sur macarte.be

Site internet prêtant assistance en cas de paiements non reconnus ou abusifs et en cas de fraude avec des cartes de crédit ou de paiement Visa ou Mastercard. Le site permet aux consommateurs de contester un achat via un formulaire et de tenter de récupérer les montants débités (pour des transactions effectuées dans un délai de moins de 3 mois).
Site internet : https://macarte.be/fr/home/help/services/purchase-dispute.html

22 Site https://cardstop.be/fr/home/Je-veux-bloquer/Bloquez-via-lemetteur.html

4 Signaler l'arnaque à Point de contact Belgique

Site internet sur lequel les consommateurs ou entreprises dont les droits n'ont pas été respectés ou les victimes de fraudes, tromperies, arnaques et escroqueries peuvent signaler leurs problèmes.

Les plaintes reçues sont analysées et le point de contact donne un avis sur mesure au consommateur et communique les signalements aux services compétents.
Site internet : https://pointdecontact.belgique.be/meldpunt/fr/bienvenue

5 Introduire une plainte auprès du bureau de police local

Il est important de veiller à mentionner dans la plainte tous les éléments possibles : les numéros de compte utilisés par le fraudeur, les en-têtes d'email, les sites internet et comptes utilisés...
Ces informations permettront à la police d'enquêter de manière optimale.

6 Signaler les contacts, sites et mails suspects au centre de la cybersécurité belge

Signaler les messages et sites suspects à l'adresse suspect@safeonweb.be afin d'éviter que d'autres personnes ne tombent dans le piège.

Ressources utiles

Nous proposons dans cette partie une boîte à outils pratiques pour :

1. Vérifier l'identité d'un interlocuteur ;
2. S'informer et prévenir les arnaques ;
3. S'assurer qu'une offre est fiable ;
4. Bloquer les appels de démarchage commercial ;
5. Contacter un organisme.

1 Vérifier l'identité d'un interlocuteur

Banque Carrefour Entreprise

Base de données du SPF Economie reprenant des informations sur les entités enregistrées et de leurs unités d'établissement.
Site internet : https://kbopub.economie.fgov.be/kbopub/zoeknummerform.html

Liste grise des télévendeurs et bureaux de recouvrement

Liste publiée sur le site du SPF Economie en collaboration avec le CEC Belgique reprenant les télévendeurs et les bureaux de recouvrement pour lesquels le SPF Economie a reçu des signalements (via Point de contact Belgique).
Site internet : https://economie.fgov.be/fr/themes/protection-des-consommateurs/arnaques-la-consommation/formes-darnaques/telephoniques/liste-des-televendeurs-et

Liste grise de la Chambre nationale des huissiers de justice

Liste des noms et adresses mails employés par des arnaqueurs pour lesquels la Chambre nationale des huissiers a reçu un signalement.
Site internet : https://www.huissiersdejustice.be/lhuissier-de-justice/informations-pratiques/fraude-internet

Liste des entreprises irrégulièrement actives en Belgique

Cette liste de la FSMA comprend :

- Des entreprises fournissant, en Belgique (ou depuis la Belgique), des services et produits financiers ne respectant pas la réglementation financière belge ;
- Des entreprises à l'égard desquelles la FSMA a constaté de sérieux indices de fraude à l'investissement ;
- Des entreprises à l'origine de fraudes de type « recovery room » (voir page 18).

Site internet : https://www.fsma.be/fr/warnings/companies-operating-unlawfully-in-belgium

Liste des personnes inscrites exerçant une activité de recouvrement amiable de dettes

Liste des recouvreurs amiables de dettes (sauf les avocats, mandataires judiciaires et officiers ministériels) inscrits auprès du SPF Economie pour exercer leur activité.
Site internet : https://economie.fgov.be/sites/default/files/Files/Publications/files/Liste-recouvreurs-de-dettes.pdf

Liste des prêteurs agréés

Liste des entreprises agréées par la FSMA pour proposer des produits financiers (prêteurs, intermédiaires en crédit hypothécaire ou à la consommation).
Site internet : https://www.fsma.be/fr/data-portal?f%5B0%5D=-fa_content_type%3Actparty#data-portal-facets

Listes de mails d'escrocs

Liste de l'asbl Neniu reprenant des adresses emails utilisées pour des escroqueries, arnaques et pièges via internet.
Site internet : https://neniu-assos.org

2 Consulter les sites d'informations sur les arnaques

Application Safeonweb

Application mise en place par le Centre pour la cybersécurité permettant de rester informé de manière simple et rapide sur les cybermenaces ou des nouveaux messages de phishing.
Site internet : https://www.safeonweb.be

Avertissements de la FSMA

La FSMA publie régulièrement sur son site internet des mises en garde relatives aux offres frauduleuses d'investissement et de crédit.
Site internet : https://www.fsma.be/fr/warnings

Brochures sur les mules financières

Febelfin a publié des brochures explicatives sur les mules financières.
Pour télécharger la brochure à destination des jeunes : https://www.febelfin.be/sites/default/files/2021-11/Brochure_geldezels_jongeren_FR.pdf
Pour télécharger la brochure à destination des accompagnants, parents... : https://www.febelfin.be/sites/default/files/2021-11/Brochure_geldezels_begeleiders_FR.pdf

Evitez les pièges

Site internet sur les escroqueries en ligne (sur internet et les réseaux sociaux) et les fausses agences de recouvrement créé par le SPF Economie.

Ce site explique comment reconnaître les fraudeurs, identifier la fraude et les actions à mettre en place pour éviter de se faire arnaquer.
Site internet : https://www.evitezlespieges.be

Fraude ou arnaque aux sentiments, à la romance, à l'amitié

Page Facebook développée par l'asbl Neniu publiant régulièrement des mises en garde au sujet de fraudes et d'arnaques aux sentiments et à l'amitié.
Site internet : https://www.facebook.com/NeniuAsblVzw

Marnaque sur Facebook

Page Facebook développée par le SPF Economie publiant régulièrement des mises en garde au sujet d'arnaques en tous genres.
Site internet : https://www.facebook.com/Marnaque

Témoignages

La FSMA propose sur son site internet une série de témoignages illustrant la façon dont les fraudeurs aux investissements et au crédit travaillent. Ce site dispense des conseils pour éviter d'en être victime.
Site internet : https://www.fsma.be/fr/temoignages

Traque l'Arnaque.be

Site internet sur les escroqueries en ligne (sur internet et les réseaux sociaux) créé par le SPF Economie à l'attention des adolescents (12 – 16 ans). Le site propose, sous la forme d'un jeu vidéo, des témoignages et explications sur les différentes arnaques et des trucs et astuces pour les éviter.
Site internet : https://www.traquelarnaque.be

Trop beau pour être vrai

Ce site internet créé par le SPF Economie et la FSMA (Wikifin) a pour mission de mettre en garde contre les arnaques, les impostures et les escroqueries et d'aider les consommateurs à les éviter.
Site internet : https://tropbeaupouretrevrai.be

3 S'assurer qu'une offre est fiable

Webshop check

Site internet proposé par le CEC Belgique offrant des conseils pour effectuer des achats sur internet en toute sécurité.
Site internet : https://www.cecbelgique.be/themes/achats-sur-internet/faites-le-webshop-check

Test « Suis-je victime d'une arnaque ? »

Test composé de 9 questions proposé par la FSMA à destination des consommateurs venant de recevoir une offre d'investissement ou ayant déjà investi et souhaitant s'assurer qu'il ne s'agit pas d'une fraude.
Site internet : https://www.fsma.be/fr/attention-aux-fraudes

4 Bloquer les appels de démarchage commercial

Ne m'appelez plus

Site internet sur lequel les consommateurs peuvent s'inscrire afin de ne plus pouvoir être démarchés de manière téléphonique par les entreprises enregistrées à la fédération belge de marketing directe. Attention : seules les entreprises pour lesquelles le consommateur a marqué son accord pourraient encore le contacter.
Site internet : https://www.dncm.be/fr/

5 Qui contacter ?

Centre Européen des consommateurs (CEC)

Réseau de 30 centres européens mis en place par la commission européenne en vue de renforcer la confiance des consommateurs dans le marché interne européen et donc favoriser les achats transfrontaliers.

Le CEC Belgique est le centre de contact de référence pour les consommateurs résidant en Belgique qui ont une question/un litige en matière de droit de la consommation qui a un caractère transfrontalier.

Comment le CEC aide-t-il les consommateurs ?

1. Informations via le site internet et brochures ;
2. Conseils juridiques via la hotline disponible tous les matins du lundi au vendredi au 02/542.33.46 ;
3. Médiation après que le consommateur ait introduit une plainte[23] .

Site internet : https://www.cecbelgique.be

SPF Economie

Le SPF Economie se charge du droit économique, le droit des entreprises et des consommateurs.

Il a pour mission de créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et des services en Belgique.

Comment le SPF Economie aide-t-il les consommateurs ?

1. Informations via son site internet et brochures ;
2. Campagnes de prévention ;
3. Mises en garde sur la page facebook Marnaque[24];

23 Sur le site https://www.cecbelgique.be/complaint-wizard-page
24 https://www.facebook.com/Marnaque

4. Gère le site Point de contact Belgique[25].

Site internet : https://economie.fgov.be/fr/themes/protection-des-consommateurs/arnaques-la-consommation/formes-darnaques/arnaques-telephoniques

Febelfin

La Fédération belge du secteur financier (Febelfin) a pour mission générale de développer un secteur financier qui répond aux besoins de la société.

Afin de remplir cette mission, elle :

1. Prend position pour défendre le secteur financier ;
2. Participe aux négociations sociales ;
3. Fournit des services :
   - Informations et conseils sur son site internet ;
   - Accompagnement de projets ;
   - Formations du secteur bancaire et financier ;
4. Communique avec les membres du secteur et le grand public ;
5. Participe à des débats politiques, sociaux et éducatifs.

Comment Febelfin aide-t-elle les consommateurs ?

1. Informations via son site internet et brochures ;
2. Campagnes annuelles de prévention sur le phishing et les mules financières ;
3. Mises en garde contre d'autres types de fraudes

Site internet : http://www.febelfin.be

FSMA – WIKIFIN

La FSMA (Autorité de contrôle dans le secteur financier) veille au traitement correct et équitable du consommateur financier et à l'éducation de celui-ci (via le programme Wikifin[26]).

25 Site https://pointdecontact.belgique.be/meldpunt/fr/bienvenue
26 Site http://www.wikifin.be

Comment la FSMA aide-t-elle les consommateurs victimes d'arnaques et d'offres frauduleuses :

1. Contribue au respect des règles visant à protéger les utilisateurs de produits ou services financiers et les emprunteurs contre l'offre ou la fourniture illicite de ceux-ci ;
2. Traiter les signalements de consommateurs en matière d'offres irrégulières de services et de produits financiers, y compris les fraudes à l'investissement et au crédit ;
3. Publie régulièrement des mises en garde[27] sur son site internet ;
4. Prend contact avec les autorités judiciaires.

Site internet : http://www.fsma.be

Neniu asbl

L'ASBL a pour mission :

- D'aider les victimes d'arnaques sur internet ;
- De donner toute l'aide possible ;
- Donner des séances d'information afin que moins de personnes ne tombent dans le piège.

Neniu publie également une liste de mails utilisés pour des escroqueries, arnaques, pièges.

Site internet : https://www.neniu-assos.org

Test-Achats

En tant qu'association de consommateurs, Test-Achats a pour mission d'informer, de servir, de défendre et de représenter les consommateurs de manière parfaitement indépendante.

27 Site https://www.fsma.be/fr/warnings

Test-Achats représente les consommateurs et défend leurs droits auprès des autorités, des instances régionales, fédérales et internationales ainsi que des entreprises.
Il propose une ligne téléphonique de conseil et d'assistance disponible du lundi au vendredi de 9h à 16h au 02/542.33.50 ou par email via un formulaire sur son site https://www.test-achats.be.

Verbraucherschutzzentrale VoG – Association de défense des consommateurs ASBL

La Verbraucherschutzzentrale VoG offre des services dans le domaine du conseil aux consommateurs, du conseil en matière d'endettement et du développement durable en Communauté germanophone et dans les communes voisines.

Comment la VSZ aide-t-elle les consommateurs victimes d'arnaques ou de fraudes ?

1. Information sur les droits ;
2. Analyse des problèmes ;
3. Recommandations et conseils ;
4. Mise en relation avec les organismes ou autorités compétentes.

Site internet : http://www.vsz.be

L'Observatoire du Crédit et de l'Endettement

Adresse : Château de Cartier, Place du Perron, 38, 6030 Marchienne-au-Pont
Tél : 071/33.12.59 - **Fax :** 071/32.25.00
Email : info@observatoire-credit.be
Site internet : http://www.observatoire-credit.be
N°entr. : 0452.320.403 – RPM Hainaut (div. Charleroi)
IBAN : BE91 0682 4452 2576

Éditeur responsable : Vincent MAGNEE, ASBL L'Observatoire du Crédit et de l'Endettement, Château de Cartier, 38, Place du Perron, 6030 Marchienne-au-pont