

Stop Arnaques



Éditrice responsable : Séverine Waterbley - N° d'entreprise : 0314.595.348 - Réf. 152-21 - Illustrations : © Adobe Stock.com

**Allo ?
Escrocs
au bout du fil !**

Caller ID:
Scam of Fraud



Situation

Un vendeur vous a fait une superbe offre commerciale par téléphone. Mais après coup, vous ne savez pas vraiment quelle est la société qui vous a appelé, ni même les conditions exactes de l'offre. Et l'e-mail de confirmation qu'on vous a envoyé n'est pas plus clair sur ces points...

Risque

Ce genre d'opération qui promet de grosses réductions pour des hôtels ou des voyages, des échantillons de produits de beauté ou qui vous invite à tester à coût réduit voire gratuitement, les produits vendus, se révèle souvent trop belle pour être vraie. Méfiance !

Même si vous avez contesté l'offre, les escrocs n'hésiteront pas à vous envoyer une facture, souvent supérieure au prix annoncé, ou à vous faire menacer par un bureau d'encaissement. Même en payant, vous risquez de ne jamais recevoir ce qu'on vous a vendu !

Conseil

Un vendeur par téléphone doit dès le début de son appel se faire connaître. Consultez la liste des sociétés de télémarketing douteuses sur le site du SPF Economie.

Il doit aussi mentionner clairement toutes les caractéristiques de son offre, vous la confirmer par écrit ou par e-mail (vérifiez toujours votre boîte spam !) et vous indiquer que vous avez un droit de rétractation de 14 jours à dater de la réception du produit vendu.

Ne vous laissez pas intimider par un bureau d'encaissement ! Contestez, le cas échéant, la validité du contrat par e-mail ou par courrier recommandé.

Et pour ne plus recevoir d'appels de télémarketing, inscrivez-vous sur la liste
« Ne m'appellez plus ».

Tombé dans le piège ?

Signalez la fraude sur : pointdecontact.belgique.be
(option « Vente par téléphone » ou « Agence de recouvrement »).

Si le vendeur est basé dans un autre pays de l'Union européenne, contactez le Centre européen des Consommateurs.

Bureaux de recouvrement et huissiers fictifs



Situation

Vous êtes contacté par un bureau de recouvrement ou un huissier qui vous réclament de l'argent pour des frais ou une dette concernant une transaction dont vous n'avez a priori pas connaissance.

Risque

Des escrocs se font régulièrement passer pour ce genre d'intermédiaires. Ils peuvent être très agressifs. Sous la pression et leurs intimidations, vous risquez de payer ce qu'ils vous réclament pour éviter des poursuites plus importantes...

Conseil

Seuls les bureaux de recouvrement et huissiers officiels peuvent agir en Belgique. Vérifiez si votre interlocuteur figure sur la liste des personnes inscrites en tant que recouvreur de dettes (disponible sur le site du SPF Economie).

Si l'histoire qu'on vous raconte ne vous dit rien, si l'on ne vous a pas envoyé de courrier auparavant ou si l'on vous demande des informations privées ou de payer sur un compte à l'étranger, soyez sur vos gardes !

Et ne vous laissez jamais intimider !

Tombé dans le piège ?

Déposez plainte auprès de la police locale.

Signalez la fraude sur pointdecontact.belgique.be (option « Agence de recouvrement »).

Microsoft a détecté des problèmes sur votre PC



Situation

Vous recevez un appel téléphonique en anglais d'une personne qui prétend travailler pour le support technique de Microsoft. Elle vous dit que de nombreux problèmes avec le système d'exploitation Windows de votre PC ont été détectés. Votre ordinateur serait infecté par des virus mais la personne vous propose son aide pour les résoudre.

Risque

Microsoft ne contacte jamais ses clients directement par téléphone. Seuls des escrocs le font en se faisant passer pour cette société. Ils sont convaincants et tenaces : même si vous raccrochez, votre interlocuteur insiste et vous rappelle pour vous persuader. Si vous doutez de ce qu'il dit, il affirme pouvoir vous prouver qu'il a bien identifié votre PC en vous faisant faire une série d'actions hors ligne sur votre ordinateur pour révéler le prétendu numéro unique d'identification de votre machine, le CLSID. Mais en réalité, ce numéro est le même pour tous les ordinateurs dotés de Windows.

Votre interlocuteur vous proposera ensuite d'installer contre une somme modique (7 ou

10 euros par exemple), un logiciel de sécurité pour nettoyer votre machine. En réalité, il s'agit d'un logiciel espion qui lui permettra de contrôler à distance votre ordinateur, d'intercepter vos mots de passe ou vos données bancaires et de vider vos comptes bancaires.

Conseil

Ne faites jamais confiance à une personne qui vous appelle au nom d'une société telle que Microsoft. Microsoft ne peut en aucune manière détecter les problèmes de votre PC à distance.

Méfiez-vous également des tentatives similaires par e-mail au nom de Microsoft.

Prétendez que vous ne parlez pas anglais et raccrochez. Tenez bon, même si on vous rappelle.

Ne communiquez aucune donnée personnelle, ni donnée bancaire (mots de passe, numéro de compte bancaire...) et ne payez rien.

Réfléchissez toujours à deux fois avant d'installer des logiciels proposés par des inconnus ou de cliquer sur un lien dans un e-mail.

Ne donnez jamais le contrôle de votre ordinateur à un inconnu.

Tombé dans le piège?

Changez tous vos mots de passe.

Si vous avez payé quelque chose, contactez immédiatement votre banque pour tenter d'annuler la transaction.

Si vous avez communiqué votre numéro de carte, appelez Card Stop (078 170 170) pour la faire bloquer.

Déposez plainte auprès de la police locale.

Alertes SMS : la facture peut vite monter



Situation

Par SMS, on vous propose des sonneries et des fonds d'écran à gogo.

Risque

En acceptant cette offre, vous acceptez peut-être aussi sans vous en rendre compte un abonnement pour des téléchargements répétitifs moyennant paiements.

Conseil

Plus que jamais, soyez vigilant : cliquer, c'est payer.

Vérifiez toujours ce à quoi vous vous engagez.

Le commerçant doit toujours prévoir un moyen pour vous désabonner. Par exemple, par un SMS « STOP » à envoyer au n° #####

Tombé dans le piège ?

Si aucun numéro n'est prévu pour vous désabonner, contactez votre opérateur téléphonique.

Si rien ne change, prévenez l'Inspection économique :
pointdecontact.belgique.be

Arnaque aux numéros surfacturés



Situation

Vous recherchez l'âme sœur et vous vous êtes enregistré(e) sur un site de rencontres. Pour rencontrer des personnes répondant à vos critères, vous devez appeler le n° 0900#####.

Risque

Vos appels téléphoniques peuvent vous revenir très cher. Certains de ces sites emploient des personnes pour vous tenir le plus longtemps possible au bout du fil.

Il arrive parfois que cette « personne » est en réalité un robot qui vous donne des réponses préprogrammées pour entretenir la conversation.

Conseil

Fort heureusement, tous les sites de rencontres ne sont pas des arnaques. Certains ont pignon sur rue. Voyez quelle est leur réputation sur les forums.

Méfiez-vous des conversations qui durent : ça coûte très cher au final !

Tombé dans le piège ?

Prévenez l'Inspection économique : pointdecontact.belgique.be

Arnaque aux droits d'auteur



Situation

Un avocat vous appelle : son client lui a signalé que vous aviez téléchargé illégalement certaines de ses œuvres sur internet. Il vous propose de régler les droits d'auteurs à l'amiable pour vous éviter un procès en justice.

Risque

Vous avez probablement affaire à un faux avocat !

Les questions de paiement de droits d'auteurs ne se règlent jamais directement avec l'artiste concerné. Aucun avocat digne de ce nom ne vous proposerait de régler un litige de la sorte.

Accepter la transaction financière proposée, c'est céder à une intimidation et perdre votre argent à coup sûr.

Conseil

Un litige de droits d'auteurs ne se règle jamais par une transaction financière discrète « à l'amiable » proposée par e-mail ou par téléphone.

N'entrez tout simplement pas dans ce jeu : c'est un piège !

Et pour éviter tout souci, ne téléchargez rien illégalement sur internet.

Tombé dans le piège ?

Déposez plainte auprès de la police locale.

Signalez la fraude sur pointdecontact.belgique.be

Déjà arnaqué, les escrocs vous proposent leur aide



Situation

Il y a quelques mois, on vous a vendu du vin par téléphone... Vous l'avez payé mais vous n'en avez jamais vu la couleur !

Aujourd'hui, un avocat vous appelle et vous signale que les malfrats ont été arrêtés au Maroc. Il vous propose de vous représenter au tribunal local afin de faire valoir vos droits.

Risque

Les arnaqueurs ne reculent devant rien ! Après le faux vin, vous avez probablement affaire à un faux avocat.

Il y a de fortes chances qu'il vous demande de payer une avance d'honoraires sur un compte à l'étranger ou via un système de paiement international. Dans ce cas, fuyez ! Aucun avocat digne de ce nom ne vous proposerait de le régler de la sorte.

Ne vous faites pas avoir deux fois par la même bande d'escrocs !

Conseil

Ne donnez pas suite à ce type d'appel car vous n'avez pratiquement aucun espoir de pouvoir récupérer votre argent par la suite.

Pour aider la police à remonter la filière et mettre fin aux activités criminelles de cette organisation internationale, relevez un maximum d'informations lors de l'appel téléphonique, par exemple : le numéro, la date et l'heure de l'appel, le nom et la fonction de la personne qui a appelé, le montant à verser, le nom et l'adresse du destinataire...

Ceci vaut également en cas de tentative d'escroquerie par internet.

Tombé dans le piège ?

Déposez plainte auprès de la police locale.

Signalez la fraude sur pointdecontact.belgique.be

Sextorsion : votre vie secrète mise à nu

Situation

Vous recevez un e-mail : « J'ai piraté votre système d'exploitation et j'ai jeté un œil sur les sites que vous visitez régulièrement... les sites pour adultes. J'ai aussi utilisé la caméra de votre ordinateur pour vous filmer. Vous êtes un grand pervers ! Vous ne voudriez pas que je montre ces images à vos parents, amis ou collègues... ».

Risque

Ce type de message est une arnaque de type « sextorsion » : les escrocs vous font croire qu'ils disposent de données ou d'images compromettantes vous concernant et vous réclament de l'argent pour ne pas les diffuser. Ils laissent même parfois entendre qu'ils ont la possibilité de bloquer votre PC et qu'il est inutile de changer de mot de passe car ils vous suivent en permanence.

Conseil

Dans la plupart des cas, les escrocs se sont procuré votre adresse e-mail par des bases de données publiques et non en infiltrant votre ordinateur. Rassurez-vous : des images, ils n'en ont pas. Ne cédez pas à leur chantage !

Par contre, le fait d'avoir reçu ce message doit vous inciter à prendre quelques précautions de base. En particulier, modifiez votre mot de passe et activez la validation en deux étapes pour tous vos comptes. Faites également une analyse approfondie de votre ordinateur avec votre antivirus. Ce n'est jamais inutile !

Tombé dans le piège ?

Déposez plainte auprès de la police locale.

Signalez la fraude sur pointdecontact.belgique.be

Une célébrité vous recommande un placement juteux

Situation

Sur internet, vous trouvez un article dans lequel un animateur télé, une star de cinéma ou un homme politique vante les mérites d'un placement qui lui a rapporté beaucoup d'argent en très peu de temps. C'est assurément une occasion à ne pas manquer...

Risque

Ce type d'annonce est très fréquent. Le problème, c'est que les personnalités qui sont mises en scène ne sont absolument pas les auteurs des annonces. Des escrocs ont usurpé leur identité et utilisent une de leurs photos pour promouvoir un investissement financier, souvent en cryptomonnaie, qui n'existe pas en réalité.

En employant l'image de ces personnalités, ils cherchent à susciter de l'intérêt pour leur proposition financière frauduleuse et à la rendre crédible. Dès que vous aurez investi dans ce prétendu placement à ne pas rater, les escrocs disparaîtront dans la nature avec votre argent.

Et comme dans la plupart des cas, vous leur aurez aussi donné vos coordonnées person-

nelles ou bancaires pour finaliser la transaction, ils auront la possibilité de s'en servir pour vider votre compte bancaire ou pour escroquer d'autres personnes à l'aide de votre identité.

Conseil

Soyez vigilant : si une offre vous paraît trop belle pour être vraie, c'est souvent qu'elle ne l'est pas, même si c'est une célébrité qui vous le dit.

Vérifiez toujours sur le site internet de la célébrité si c'est bien elle qui recommande le placement. Et même si elle est bien à l'origine de cette recommandation, dites-vous qu'elle n'est pas spécialiste en investissements financiers.

Cherchez toujours à en savoir plus à propos de l'intermédiaire financier et de l'offre présentée. Si les choses ne sont pas claires, fuyez !

Ne communiquez jamais vos coordonnées bancaires ou des copies de vos documents d'identité à des intermédiaires obscurs.

Ne cliquez pas sur les liens qui pourraient se trouver dans l'article que vous avez lu ou dans un e-mail qu'on vous aurait envoyé.

Tombé dans le piège ?

Stoppez tout contact avec vos interlocuteurs. Ne payez plus rien !

Prévenez votre banque de toute urgence !

Si vous avez communiqué votre numéro de carte, appelez Card Stop (078 170 170) pour la faire bloquer.

Déposez plainte auprès de la police locale.

Signalez la fraude sur pointdecontact.belgique.be

Quand les voleurs se font passer pour Interpol



Situation

Vous avez été victime d'une fraude à l'amitié. Sur internet, vous lisez le témoignage de quelqu'un qui, dans le même cas que vous, a réussi à récupérer l'argent perdu grâce à Interpol. L'adresse e-mail à contacter est indiquée.

Risque

L'adresse e-mail est fausse : elle n'a rien à voir, ni avec Interpol, ni avec la police.

Si vous contactez cette adresse, quelqu'un va essayer d'obtenir vos coordonnées bancaires, soi-disant pour vous verser les fonds récupérés mais ce sera en fait pour vous arnaquer une deuxième fois.

Conseil

Dites-vous bien que vous ne reverrez sans doute plus jamais l'argent que vous avez perdu dans une fraude à l'amitié.

Méfiez-vous des témoignages mentionnant des adresses e-mail miracles ou le nom d'organismes tels que Interpol ou la police, surtout quand ce nom apparaît avant le symbole « @ » (p. ex. : commissaireinterpol@cyberservices.com).

Ne communiquez en aucun cas vos coordonnées personnelles et bancaires.

Tombé dans le piège ?

Prévenez votre banque de toute urgence !

Déposez plainte auprès de la police locale.

Signalez la fraude sur pointdecontact.belgique.be

Arnaque au RGPD : vos données personnelles en danger

GDPR

Situation

Vous êtes une entreprise et vous avez reçu une lettre ou un e-mail vous invitant à faire un paiement à une organisation inconnue qui serait responsable de l'application du règlement général sur la protection des données (RGPD).

Risque

Ce message est probablement une tentative d'arnaque afin de vous extorquer de l'argent ou de vous voler vos données bancaires et professionnelles.

En aucun cas, une instance officielle telle que l'Union européenne p. ex., ne demande de communiquer des mots de passe ou des données bancaires ou personnelles par e-mail, par SMS ou par téléphone.

Conseil

De tels courriers ou e-mails ont un caractère très professionnel mais leur apparence officielle (logo de l'Union européenne, message en anglais, etc.) ne doit pas vous influencer.

Soyez extrêmement vigilant et vérifiez toujours de qui émane le message.

En aucun cas, ne communiquez des données confidentielles de votre entreprise. Et n'oubliez pas de sensibiliser tout votre personnel à une possible tentative d'escroquerie de ce genre.

Tombé dans le piège ?

Prenez contact avec votre banque.

Déposez plainte auprès de la police locale.

Signalez la fraude sur pointdecontact.belgique.be

Vente en **seconde main** : **les escrocs** saisissent **l'occasion**



Situation

Vous avez mis en vente un objet sur un site d'objets de seconde main. Quelqu'un vous contacte et vous propose un prix très élevé, à condition que la transaction se fasse via un autre site.

Risque

Les escrocs vont vous demander de communiquer vos coordonnées bancaires pour le paiement via cet autre site. Toutefois, vous ne verrez jamais l'argent arriver sur votre compte. Au contraire, vous risquez de vous faire dévaliser.

Et si vous avez expédié votre objet, lui aussi sera perdu.

Conseil

Pour vos transactions en ligne, favorisez toujours les sites disposant d'une bonne e-réputation. Optez pour les sites qui ont pignon sur rue : souvent, ils vous offrent des garanties contre les mauvais payeurs.

Cherchez toujours à en savoir plus à propos de vos interlocuteurs.

Et la règle d'or : ne communiquez jamais vos coordonnées bancaires à des intermédiaires obscurs.

Tombé dans le piège ?

Prévenez votre banque de toute urgence !

Déposez plainte auprès de la police locale.

Signalez la fraude sur pointdecontact.belgique.be

Vente en seconde main : votre acheteur veut utiliser un service de coursier



Situation

Vous avez mis en vente un objet sur une plateforme de vente de seconde main (eBay ou Facebook Marketplace p. ex.). Une personne vous contacte très rapidement pour l'acheter mais vous dit ne pas pouvoir récupérer elle-même votre produit. Elle vous propose de faire appel à un service de livraison connu (Mondial Relay, DPD, DHL, GLS...) et de vous payer via ce service.

Risque

Les escrocs vous servent généralement une excuse pour vous inciter à vous diriger sur un autre site web que la plateforme bien connue et fiable que vous avez choisie.

Les escrocs utilisent des reproductions frauduleuses de sites web. Ces faux sites vous renvoient ensuite vers une copie du site web de votre banque en ligne, où vous êtes invité à saisir vos informations de paiement. En procédant de la sorte, vous donnez à votre interlocuteur l'accès à vos comptes bancaires et vous risquez de vous faire dévaliser.

Parfois, les escrocs vous appellent au nom de la société de livraison pour soi-disant valider votre identité avec votre digipass. Ils peuvent aussi recourir à de faux e-mails de confirma-

tion qui ressemblent à ceux employés par votre plateforme de vente officielle.

Et si vous expédiez votre objet, vous ne le reverrez plus..

Conseil

Que vous vendiez ou achetiez via des plateformes en ligne, soyez toujours sur vos gardes dès que votre interlocuteur vous demande de sortir de la plateforme pour finaliser la vente ou l'achat.

Pour vos transactions en ligne, favorisez toujours les services proposés directement par la plateforme de vente que vous avez choisie et disposant d'une bonne e-réputation.

Ne cliquez jamais sur un lien que l'acheteur vous transmettrait par e-mail et insistez pour finaliser la commande par vous-même via la plateforme de votre choix. Les plateformes qui ont pignon sur rue, vous offrent des garanties contre les mauvais payeurs.

Ne payez jamais rien, quelle que soit la raison invoquée par l'acheteur : si c'est vous qui vendez, il n'est pas normal que vous deviez payer quelque chose, même si c'est un tout petit montant.

Et surtout, ne communiquez jamais vos coordonnées bancaires à des intermédiaires obscurs.

Tombé dans le piège ?

Prévenez votre banque de toute urgence !

Déposez plainte auprès de la police locale et de votre plateforme de vente.

Signalez la fraude sur pointdecontact.belgique.be

Lettre nigériane : quelqu'un a de l'argent bloqué et demande votre aide pour le débloquer



Situation

Vous recevez un e-mail d'une personne inconnue qui vous demande de l'aider à récupérer des capitaux importants lui appartenant, bloqués dans un pays étranger.

Pour vous remercier de votre aide, elle vous promet 10 % de la somme totale.

Risque

Si vous répondez au message et communiquez vos coordonnées, les arnaqueurs vous recontacteront en vous demandant de payer des frais de dossier, des taxes diverses, etc. sous prétexte de débloquer l'argent.

Cet argent n'existe évidemment pas et vous n'en verrez jamais les 10 % !

Conseil

Il n'est pas logique qu'un inconnu sollicite votre assistance dans le cadre de transfert de fonds. Pourquoi vous ? Où a-t-il trouvé vos coordonnées ?

Ne donnez jamais suite à ce genre de demande ! Ne communiquez aucune donnée personnelle, et surtout ne payez rien !

Si le message est truffé de fautes d'orthographe, c'est souvent le signe d'une escroquerie menée depuis l'étranger. Ces messages sont toutefois rédigés de manière de plus en plus professionnelle et sont donc plus difficiles à reconnaître.

Tombé dans le piège ?

Prévenez l'Inspection économique : pointdecontact.belgique.be

Placement en **diamants** : un **choix** pas toujours **brillant** !

Situation

INCROYABLE : les banques cachent la vérité aux Belges ! Savez-vous qu'il est possible de placer votre argent à un taux de 8 % dans le diamant ? C'est en tout cas ce que vous avez lu sur internet...

Risque

Placer son argent dans des biens physiques tels que des diamants, des métaux précieux ou des terres rares constitue une alternative extrêmement risquée aux produits d'épargne classiques. Les rendements annoncés ne sont pas garantis : votre capital est en jeu, sans oublier que dans la pratique, les faux et les arnaques sont fréquents !

Conseil

Vendre des diamants comme un investissement n'est pas illégal en soi mais il existe des règles strictes pour les présenter comme un placement financier. Ne vous laissez pas abuser par le côté attractif et faussement rassurant de certaines annonces.

De plus, la vente de certains de ces produits est réservée à des personnes déterminées et est soumise à des conditions particulières.

Et comme vous n'êtes pas un expert en la matière, méfiez-vous des faux diamants (ou des pièces et lingots à la teneur en or trafiquée). Choisissez de préférence un diamantaire belge figurant sur le site web www.awdc.be.

En cas de doute concernant une offre d'investissement financier, faites-la vérifier par l'autorité de surveillance des marchés financiers (FSMA).

Tombé dans le piège ?

Déposez plainte auprès de la police locale.

Signalez la fraude à la FSMA.

Infos sponsorisées sur internet : abonnements cachés



Situation

Dans la presse, vous découvrez les coordonnées d'un site internet donnant des conseils diététiques.

Vous tapez l'adresse de ce site et vous cochez la case prévue pour recevoir par e-mail leur lettre « Votre santé au quotidien ».

Risque

L'objectif est de vous piéger et de vous faire conclure un abonnement pour des services souvent sans valeur.

Sauf mention contraire, vos coordonnées peuvent être analysées et revendues à des

sociétés de marketing qui vous inondent de publicités correspondant à vos habitudes supposées. Ces annonceurs non désirés sont peut-être mal intentionnés : virus informatiques, vol de données bancaires...

Conseil

Lisez les petits caractères avant de taper « OK » pour souscrire à de telles lettres d'information.

Ne communiquez pas votre numéro de carte de crédit ou vos coordonnées bancaires dans de telles circonstances.

Tombé dans le piège ?

Prévenez l'Inspection économique : pointdecontact.belgique.be

Alerte virus sur votre ordinateur



Situation

Vous surfez tranquillement sur votre PC, votre tablette ou votre smartphone quand soudain apparaît une page avec le logo « Google » indiquant que 4 virus ont été détectés sur votre appareil. Vous avez 2 minutes pour le nettoyer gratuitement, en cliquant sur le bouton figurant en bas de la page.

Risque

Quelqu'un essaie de se faire passer pour « Google » dans le but de vous voler vos coordonnées ou d'accéder frauduleusement à votre ordinateur.

Cliquer sur le bouton, c'est courir le risque qu'on usurpe votre identité, voire vos données bancaires ou que l'on accède à votre ordinateur.

Conseil

Ne donnez pas suite à ce message : fermez la page ou mieux, éteignez et relancez votre appareil !

Ne cliquez jamais sur les liens et autres boutons présents dans de tels messages et n'ouvrez pas les éventuels documents joints. Ils contiennent peut-être des logiciels espions.

Protégez-vous à l'aide d'un bon antivirus et pensez à changer régulièrement vos mots de passe.

Tombé dans le piège ?

Déposez plainte auprès de la police locale.

Informez l'Inspection économique : pointdecontact.belgique.be

Si vous avez communiqué vos données bancaires, prévenez également votre banque !

Arnaque aux faux médicaments



Situation

Vous envisagez d'acheter des médicaments via internet. D'après la publicité, ils sont tout aussi efficaces et bien moins chers que chez votre pharmacien.

Risque

Les produits de santé vendus sur internet ne sont pas tous certifiés par l'industrie pharmaceutique.

Vous ne savez pas d'où proviennent ces médicaments, ni s'ils sont authentiques (contrefaçons). Dans le doute, abstenez-vous !

L'utilisation de produits de santé sans conseil avisé n'est pas sans risques.

Conseil

Parlez-en à votre médecin ou à votre pharmacien. Demandez-leur ce qu'ils pensent de ces produits. Il est possible après tout que ces produits soient efficaces et vendus sur des sites internet fiables.

Tombé dans le piège ?

Contactez l'Agence fédérale des médicaments et des produits de santé :
www.afmps.be

Facturé pour une commande en ligne que vous n'avez jamais passée (swipe)

Situation

Vous recevez une facture pour des articles achetés sur une plateforme en ligne. Pourtant, vous en êtes sûr, vous n'avez rien commandé et rien reçu.

Risque

Des escrocs se sont emparés de vos identifiants sur une plateforme de commerce électronique. Ils ont passé une grosse commande à votre nom et l'ont fait livrer à une autre adresse ou dans un point de distribution automatique.

Comme ils ont demandé à payer après livraison, vous recevez la facture mais la marchandise a déjà été récupérée par des complices qui ont disparu dans la nature.

Conseil

Pour toutes vos transactions en ligne, sécurisez au maximum votre compte. Privilégiez l'identification à deux facteurs. Et si elle n'est pas proposée par la plateforme de commerce électronique, choisissez un mot de passe compliqué. Et n'oubliez pas qu'un mot de passe est et doit rester secret !

Pensez aussi à changer régulièrement votre mot de passe. Les identifiants et les mots de passe sont des données qui s'échangent ou se vendent très facilement entre escrocs.

N'oubliez pas que vous disposez d'un droit de rétractation de 14 jours pour tout achat à distance effectué dans l'Union européenne. Dès que vous recevez le message de confirmation de votre prétendue commande, signalez au vendeur que vous n'avez rien commandé et que vous renoncez à la marchandise.

Et si on livre chez vous des articles au nom d'une personne que vous ne connaissez pas, refusez-les ou portez-les à la police.

Tombé dans le piège ?

Prévenez au plus vite la plateforme de vente que vous renoncez à l'achat.

Déposez plainte auprès de la police locale.

Signalez la fraude sur pointdecontact.belgique.be

Fraude à la facture : vous avez payé mais le vendeur n'a rien reçu

Situation

Vous avez fait installer une nouvelle cuisine et vous avez reçu la facture du fournisseur. Vous virez le montant sur le numéro de compte mentionné sur la facture, mais quelques semaines plus tard, vous recevez un rappel de paiement dans votre boîte aux lettres.

Risque

Votre facture a probablement été falsifiée. Dans le cas de cette fraude, des arnaqueurs interceptent les factures papier (ou électroniques), changent le numéro de compte et les envoient ainsi modifiées. Lorsque vous effectuez votre paiement, vous payez donc les arnaqueurs. Vous courez donc le risque de devoir payer deux fois la facture parce que votre fournisseur n'a reçu aucun paiement.

Conseil

Comparez le numéro de compte figurant sur votre facture avec celui mentionné sur le bon de commande ou sur le site internet officiel de votre fournisseur.

Soyez vigilant lorsqu'une facture mentionne un nouveau numéro de compte ou si c'est la première fois que vous payez ce fournisseur.

En cas de doute, appelez l'entreprise via un numéro que vous connaissez déjà (le numéro de téléphone sur la facture peut également avoir été falsifié).

Tombé dans le piège ?

Contactez le plus rapidement possible les banques concernées afin de signaler la fraude.

Signalez la fraude sur pointdecontact.belgique.be (option « factures falsifiées »).

Fraude à la facture : votre client a payé mais vous n'avez rien reçu

Situation

Vous êtes entrepreneur et vous effectuez des travaux de transformation chez des clients. Vous envoyez vos factures, mais les paiements se font attendre. Après avoir adressé des rappels à quelques clients, vous apprenez qu'ils ont bel et bien payé, mais pas sur votre compte en banque.

Risque

Vos factures ont probablement été falsifiées. Dans le cas de cette fraude, des arnaqueurs interceptent les factures papier (ou électroniques), changent le numéro de compte et les envoient ainsi modifiées. Lorsque le client effectue le paiement, il paie donc les arnaqueurs. Le risque est que votre client ne soit plus en mesure de vous payer étant donné qu'il a déjà viré l'argent (sur le mauvais compte).

Conseil

Indiquez votre numéro de compte sur vos factures, mais aussi sur vos bons de commande et sur votre site internet.

Demandez à vos clients de vérifier le numéro de compte avant qu'ils n'effectuent leur paiement.

Sur vos enveloppes, évitez des mentions qui pourraient attirer l'attention des arnaqueurs. Utilisez par exemple des enveloppes blanches sans fenêtre.

Tombé dans le piège ?

Demandez à votre client de contacter le plus rapidement possible sa banque afin de signaler la fraude.

Signalez la fraude sur pointdecontact.belgique.be (option « factures falsifiées »).

Fraude à l'amitié



Situation

Vous étiez à la recherche d'un partenaire ou d'un ami sur Facebook, ou via une application en ligne ou un site de rencontres, et vous venez de trouver la perle rare... A priori tout colle entre vous mais votre prince charmant (ou votre belle princesse) ne tarde pas à vous demander des cadeaux, vos informations personnelles et surtout, de l'argent.

Risque

Toutes les rencontres sur internet ne sont pas des arnaques mais les fraudes à l'amitié sont très nombreuses et fonctionnent toutes selon le même schéma : un escroc joue avec vos sentiments et vous demande de l'argent afin de financer son voyage vers la Belgique pour vous rencontrer, prendre soin de sa famille laissée au pays, couvrir des frais d'hospitalisation ou de scolarité, débloquer un héritage, etc.

Laissez-vous apitoyer et après quelques versements, vous n'aurez tout à coup plus aucune nouvelle, ni de la personne, ni de votre argent.

Conseil

Il n'y a pas de mal à discuter sur internet mais ne communiquez aucune information sensible vous concernant.

Vérifiez toujours l'authenticité du profil de la personne. Souvent les escrocs utilisent de faux profils ou des profils usurpés.

Ne vous faites pas avoir par des histoires à pleurer.

Et ne payez jamais rien tant que vous n'avez pas rencontré physiquement la personne car l'argent versé ne se revoit jamais !

Tombé dans le piège ?

Prévenez votre banque de toute urgence !

Signalez la fraude sur pointdecontact.belgique.be

Apps et Réseaux sociaux : attention aux faux amis ! (whaling)

Situation

Ce matin, vous avez reçu, via Facebook ou une app telle que Whatsapp, un message d'une de vos proches en vacances à l'étranger. Pas de chance ! La pauvre s'est fait voler son portefeuille et elle vous demande de lui envoyer un peu d'argent pour l'aider...

Risque

Il est fort possible que ce message ne vienne pas de votre amie. Un escroc peut lui avoir piraté son compte Facebook, Instagram ou Whatsapp et se fait passer pour elle pour vous extorquer de l'argent en jouant sur votre émotion.

Conseil

Méfiez-vous des demandes d'argent urgentes via un numéro de téléphone inconnu, une app ou un média social.

Vérifiez toujours à qui vous avez affaire en contactant votre interlocuteur par un autre canal.

Ne versez jamais d'argent sur un compte inconnu ou appartenant à une tierce personne.

Tombé dans le piège ?

Stoppez tout contact avec les escrocs.

Si vous avez payé, prévenez votre banque.

Rassemblez un maximum de preuves (captures d'écran p. ex.).

Déposez plainte auprès de la police locale.

Informez l'Inspection économique : pointdecontact.belgique.be

On vous demande de confirmer une commande que vous n'avez pas passée

Situation

Vous recevez un e-mail vous confirmant que votre commande a bien été exécutée.

Le message vous invite, si vous n'avez passé aucune commande, à le signaler en cliquant sur un lien.

Or, vous n'avez jamais passé une telle commande...

Risque

Quelqu'un essaie de vous voler vos coordonnées ou d'accéder frauduleusement à votre ordinateur.

Répondre à cet e-mail, c'est courir le risque qu'on usurpe votre identité, voire vos données bancaires, ou que l'on accède à votre ordinateur.

Conseil

Ne donnez pas suite à cet e-mail : détruisez-le !

Ne cliquez pas sur les liens présents dans le message et n'ouvrez pas les éventuelles pièces jointes. Elles contiennent peut-être des logiciels espions.

Tombé dans le piège ?

Transférez le message à suspect@safeonweb.be

Si vous avez communiqué vos données bancaires, prévenez immédiatement votre banque !

Déposez plainte auprès de la police locale si de l'argent a disparu de votre compte.

Informez l'Inspection économique : pointdecontact.belgique.be

Si vous ne parvenez pas à un accord avec votre banque, informez l'Inspection économique (pointdecontact.belgique.be) et faites appel à l'Ombudsfin, le Service de médiation pour les conflits financiers.

Une facture à payer en scannant un code QR (quishing)



Situation

Vous recevez un message par e-mail vous invitant à payer une facture grâce à un code QR.

Risque

Vous avez peut-être affaire à une tentative d'arnaque appelée « quishing ».

Les escrocs se font souvent passer pour des organismes officiels. Ils diffusent dans des e-mails, des SMS ou des messages WhatsApp, des codes QR qui, lorsque vous les scannez, vous dirigent vers des sites où, soit on tentera de voler vos coordonnées bancaires (phishing), soit on vous invitera à effectuer un paiement.

Les codes QR sont également utilisés pour installer des logiciels malveillants sur les ordi-

nateurs des victimes afin de voler des données personnelles, leurs identifiants de connexion...

Conseil

Il est très difficile d'identifier un code QR frauduleux. Ce qui doit vous mettre la puce à l'oreille, c'est le contenu du message dans lequel se trouve le code. Par exemple, si l'on vous demande de payer une facture dont vous n'avez pas connaissance, ce n'est pas normal !

En cas de doute, ne scannez pas le code QR. Transférez le message frauduleux à **suspect@safeonweb.be** et supprimez-le.

Et si par mégarde, vous avez scanné le code, ne communiquez aucune donnée personnelle.

Tombé dans le piège ?

Transférez le message à **suspect@safeonweb.be**

Si vous avez communiqué vos données bancaires, prévenez immédiatement votre banque !

Déposez plainte auprès de la police locale si de l'argent a disparu de votre compte.

Informez l'Inspection économique : **pointdecontact.belgique.be**

Si vous ne parvenez pas à un accord avec votre banque, informez l'Inspection économique (**pointdecontact.belgique.be**) et faites appel à Ombudsfm, le Service de médiation pour les conflits financiers.

**Bonne nouvelle :
vous avez gagné
sans jouer**



Situation

Ça y est ! Vous avez gagné à la loterie !

C'est en tout cas ce que dit l'e-mail que vous venez de recevoir.

Il ne vous reste plus qu'à payer les modestes frais de transaction pour recevoir votre lot...

Risque

Ces messages sont envoyés à des milliers de personnes.

En réalité, vous n'êtes pas le grand gagnant. Au contraire, si vous payez la somme demandée, vous serez à tous les coups... perdant.

Conseil

Si vous n'avez participé à aucune loterie, vous ne pouvez pas avoir gagné : ne répondez pas !

Ne communiquez jamais vos coordonnées bancaires.

Tombé dans le piège ?

Transférez le message à suspect@safeonweb.be

Si vous avez communiqué vos données bancaires, prévenez immédiatement votre banque !

Déposez plainte auprès de la police locale si de l'argent a disparu de votre compte.

Informez l'Inspection économique : pointdecontact.belgique.be

Si vous ne parvenez pas à un accord avec votre banque, informez l'Inspection économique (pointdecontact.belgique.be) et faites appel à Ombudsfm, le Service de médiation pour les conflits financiers.

Faux message de votre banque



Situation

Vous recevez un e-mail de votre banque vous demandant de vérifier vos données personnelles.

Risque

Quelqu'un essaie de vous voler vos données bancaires.

Répondre à cet e-mail, c'est courir le risque qu'on vide très rapidement votre compte.

Conseil

Une banque n'envoie jamais ce type d'e-mail, car elle dispose déjà de toutes vos données.

Ne donnez pas suite à cet e-mail : détruisez-le !

Ne cliquez pas sur les liens présents dans le message et n'ouvrez pas les éventuelles pièces jointes. Elles contiennent peut-être des logiciels espions.

Tombé dans le piège ?

Transférez le message à suspect@safeonweb.be

Si vous avez communiqué vos données bancaires, prévenez immédiatement votre banque !

Déposez plainte auprès de la police locale si de l'argent a disparu de votre compte.

Informez l'Inspection économique : pointdecontact.belgique.be

Si vous ne parvenez pas à un accord avec votre banque, informez l'Inspection économique (pointdecontact.belgique.be) et faites appel à Ombudsfin, le Service de médiation pour les conflits financiers.

Arnaque avec votre digipass

Situation

Vous avez reçu un SMS ou un e-mail vous signalant que vous avez payé deux fois une facture. Dans le message, un lien sur lequel cliquer vous redirige vers un site grâce auquel vous serez remboursé. Vous faites le nécessaire mais quelqu'un vous appelle pour vous demander de confirmer le remboursement en utilisant le lecteur de carte de votre banque.

Risque

Quelqu'un essaie de vous voler vos données bancaires pour effectuer un paiement au départ de votre compte. Si vous communiquez le code chiffré que vous indique votre lecteur de carte bancaire (digipass), vous l'autorisez à faire ce paiement dont vous ignorez même le montant. Votre compte risque d'être rapidement vidé.

Conseil

Vérifiez vos relevés bancaires. Vous verrez immédiatement s'il y a eu ou non un double paiement.

Pour procéder à un remboursement, un commerçant a juste besoin de votre numéro de compte. Et la plupart du temps, il le connaît déjà puisque vous l'avez utilisé pour payer votre facture.

Votre digipass sert à vous authentifier auprès de votre banque et à sécuriser vos paiements, jamais à recevoir de l'argent ! Ne communiquez jamais le code signature qu'il vous indique à qui que ce soit !

Tombé dans le piège ?

Transférez le message à suspect@safeonweb.be

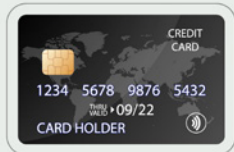
Si vous avez communiqué vos données bancaires, prévenez immédiatement votre banque !

Déposez plainte auprès de la police locale si de l'argent a disparu de votre compte.

Informez l'Inspection économique : pointdecontact.belgique.be

Si vous ne parvenez pas à un accord avec votre banque, informez l'Inspection économique (pointdecontact.belgique.be) et faites appel à l'Ombudsfin, le Service de médiation pour les conflits financiers.

Carte bancaire à renvoyer par courrier ? Jamais !



Situation

Vous recevez un message de votre banque vous signalant que votre carte de crédit doit être remplacée. On vous demande de la renvoyer par courrier à une certaine adresse.

Risque

Quelqu'un essaie de vous voler vos données bancaires.

Si vous renvoyez votre carte, votre compte sera très rapidement vidé.

Conseil

Une banque ne demande jamais de lui renvoyer une carte par courrier.

Ne donnez pas suite à ce message : détruisez-le !

Si vous l'avez reçu par e-mail, ne cliquez pas sur les liens présents dans le message et n'ouvrez pas les éventuelles pièces jointes. Elles contiennent peut-être des logiciels espions.

Tombé dans le piège ?

Transférez le message à suspect@safeonweb.be

Si vous avez communiqué vos données bancaires, prévenez immédiatement votre banque !

Déposez plainte auprès de la police locale si de l'argent a disparu de votre compte.

Informez l'Inspection économique : pointdecontact.belgique.be

Si vous ne parvenez pas à un accord avec votre banque, informez l'Inspection économique (pointdecontact.belgique.be) et faites appel à l'Ombudsfin, le Service de médiation pour les conflits financiers.

Un rendez-vous inconnu a été ajouté à votre agenda en ligne

Situation

Vous avez découvert sur le calendrier en ligne lié à votre boîte mail, un rendez-vous inscrit sans que vous en soyez l'auteur. Le message émane d'une entreprise connue et vous invite à cliquer de toute urgence sur un lien pour récupérer un cadeau.

Risque

Il s'agit probablement d'une tentative de phishing.

Les plateformes mail ne parviennent pas à détecter et filtrer les messages quand ils sont placés dans votre agenda en ligne. Clairement, quelqu'un est parvenu à s'introduire dans le vôtre et essaie de vous voler votre identité et votre argent.

Si vous cliquez sur le lien, vous serez renvoyé vers un faux formulaire de contact dans lequel on vous demandera vos coordonnées personnelles et bancaires. Gare au contenu de votre compte en banque !

Conseil

Ne donnez pas suite à ce genre de rendez-vous : supprimez-le tout simplement !

Vérifiez dans la section « spam » de votre boîte mail si vous n'avez pas également reçu une tentative d'escroquerie similaire. Si c'est le cas, supprimez également le message.

Désactivez l'acceptation automatique des rendez-vous dans les paramètres de votre agenda en ligne.

Que ce soit par téléphone, e-mail, SMS ou chat, ne communiquez jamais votre code secret, ni votre mot de passe, ni aucun code généré par votre lecteur de carte bancaire ou par votre app itisme.

Ne cliquez pas sur les liens présents dans les messages que vous recevez et n'ouvrez pas les éventuelles pièces jointes. Elles contiennent peut-être des logiciels espions.

Tombé dans le piège ?

Transférez le message du rendez-vous à suspect@safeonweb.be

Si vous avez communiqué vos données bancaires, prévenez immédiatement votre banque !

Si de l'argent a disparu de votre compte dans l'intervalle et que la banque refuse de vous rembourser, vous pouvez faire appel à Ombudsfín, le Service de médiation pour les conflits financiers.

Déposez plainte auprès de la police locale et informez l'Inspection économique : pointdecontact.belgique.be.

Votre banque vous demande de transférer votre argent pour plus de sécurité

Situation

Une personne qui prétend appartenir au service des fraudes de votre banque vous appelle. Cette personne vous explique qu'on soupçonne une fraude sur votre compte et vous recommande de transférer votre argent sur un autre compte. Pour ce faire, votre interlocuteur vous demande votre code secret et vous invite à installer un logiciel.

Risque

Quelqu'un essaie de vous voler votre argent. Jamais votre banque ne vous appellera, ni ne vous enverra un e-mail pour vous demander de transférer de l'argent.

En suivant les instructions qu'on vous donne, vous envoyez directement vos économies sur le compte des escrocs qui vous appellent.

Qui plus est, vous risquez qu'ils vous volent vos données bancaires pour vous arnaquer une deuxième fois ou piéger d'autres personnes en se servant de votre identité.

Ne donnez pas suite à ce genre de message : raccrochez ou supprimez l'e-mail !

Que ce soit par téléphone, e-mail, SMS ou chat, ne communiquez jamais votre code secret, ni votre mot de passe, ni aucun code généré par votre lecteur de carte ou par votre smartphone.

Pour exécuter vos opérations financières en ligne ou sur votre smartphone, connectez-vous toujours vous-même directement, sans passer par un lien qu'on vous aurait donné.

Ne cliquez pas sur les liens présents dans les messages que vous recevez et n'ouvrez pas les éventuelles pièces jointes. Elles contiennent peut-être des logiciels espions.

Ne laissez jamais un inconnu accéder à votre ordinateur ou vous faire installer un prétendu logiciel de sécurité.

Tombé dans le piège ?

Si vous avez reçu un message écrit, transférez-le à suspect@safeonweb.be

Si vous avez communiqué vos données bancaires, prévenez immédiatement votre banque !

Si vous ne parvenez pas à un accord avec votre banque, vous pouvez faire appel à l'Ombudsfin, le Service de médiation pour les conflits financiers.

Déposez plainte auprès de la police locale si de l'argent a disparu de votre compte et informez l'Inspection économique : pointdecontact.belgique.be

Des palettes de produits vendues à un prix dérisoire

Situation

Vous voyez un message sur Facebook : une grande enseigne (Lidl, Amazon, Brussels Airport...) doit faire de la place dans ses entrepôts. Des stocks de produits de qualité sont liquidés pour un prix ridiculement faible (moins de 2 euros). Dépêchez-vous : il ne reste que quelques palettes ! Premier arrivé, premier servi...

Risque

C'est une technique fréquente d'arnaque. On vous fait miroiter une affaire à ne pas manquer, en utilisant le nom d'une entreprise bien connue ; vous payez la petite somme demandée, parfois majorée de frais d'expédition du produit commandé... mais vous ne recevez jamais le produit en question. Et pour cause : ce produit n'existe pas !

En réalité, quelqu'un joue sur l'effet de masse pour récolter de l'argent. Beaucoup de petits montants peuvent devenir rapidement une grosse somme.

Qui plus est, vous risquez que les escrocs vous volent vos données bancaires pour tenter de vous arnaquer une deuxième fois ou pour piéger d'autres personnes en se servant de votre identité.

Conseil

Demandez-vous s'il est logique que des palettes entières de produits de valeur soient vendues à un prix aussi bas. Même en période de soldes ou lors du Black Friday par exemple, de telles démarques sont suspectes.

Recherchez des informations sur le site web de l'entreprise qui procède au prétendu déstockage. Si vous n'y trouvez rien sur cette opération, c'est que l'information est trop belle pour être vraie.

Ne payez rien et ne partagez en aucun cas vos coordonnées bancaires.

Que ce soit par téléphone, e-mail, SMS ou chat, ne communiquez jamais le code secret de votre carte bancaire, ni un mot de passe, ni aucun code généré par votre lecteur de carte bancaire ou par votre app itsme.

Tombé dans le piège ?

Si vous avez communiqué vos données bancaires, prévenez immédiatement votre banque !

Si de l'argent a disparu de votre compte dans l'intervalle et que la banque refuse de vous rembourser, vous pouvez faire appel à Ombudsfm, le Service de médiation pour les conflits financiers.

Déposez plainte auprès de la police locale et informez l'Inspection économique : pointdecontact.belgique.be

**Prix trop bas,
méfie-toi !**

**SPECIAL
OFFER**

Situation

Vu sur eBay : une voiture pour seulement 500 euros ! Et sur Kapaza : un smartphone dernier cri pour seulement quelques euros...

Risque

Ces prix bas sont destinés à attirer le client.

Il est très possible que cette voiture ou ce smartphone n'existent tout simplement pas ou qu'il s'agisse de prix de départ pour des enchères.

Il arrive aussi souvent que ces produits soient de la contrefaçon.

Conseil

Méfiez-vous des trop bonnes affaires.

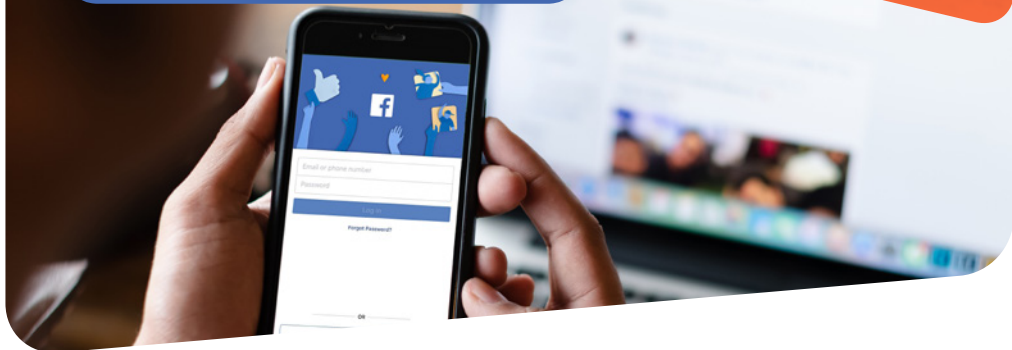
Comparez toujours le prix de vente proposé sur le site avec celui pratiqué dans le commerce.

Cela vous servira de référence en cas de vente aux enchères.

Tombé dans le piège ?

Prévenez l'Inspection économique : pointdecontact.belgique.be

Crédit via Facebook



Situation

Vous êtes attiré par une publicité sur Facebook : « Votre crédit accepté en quelques clics ! Argent libéré dès paiement des frais de dossier ».

Risque

Cette proposition est tellement simple qu'il y a de grandes chances que la seule chose qui soit vraie, ce sont les frais de dossiers que vous allez payer...

Le crédit à la consommation est une affaire sérieuse réglementée par la loi. Les véritables intermédiaires de crédit n'agissent pas via les réseaux sociaux. C'est contraire à la déontologie de leur profession.

Conseil

Aussi tentante que soit l'annonce et quelle que soit votre situation financière, ne prenez pas le risque de payer des arnaqueurs.

Ne traitez pas vos affaires d'argent sur les réseaux sociaux : ignorez ce type de publicités pour du crédit facile ! Mieux encore, évitez de cliquer sur celles-ci, sans quoi vous risquez d'être inondé d'annonces du même genre à l'avenir.

Tombé dans le piège ?

Déposez plainte auprès de la police locale.

Signalez la fraude sur pointdecontact.belgique.be

Avion bon marché ? Le prix peut vite s'envoler



Situation

Sur internet, vous découvrez des billets d'avion extrêmement bon marché.

Risque

Le prix final peut s'avérer bien plus élevé que celui que vous avez vu au départ.

En effet, selon le jour et l'heure de votre vol, le prix va varier. De même, certains services peuvent être en option et payants : bagages, assurance, choix du siège, embarquement prioritaire, repas, mode de paiement...

Conseil

Ne prenez pas pour argent comptant le prix que vous voyez sur la première page du site internet.

Faites une simulation complète en fonction des services que vous souhaitez, et faites jouer la concurrence.

Tombé dans le piège ?

Vous ne devez rien faire car a priori, rien n'est illégal dans cette situation.

Si toutefois, vous jugez que l'information sur le site est trompeuse pour le consommateur, prévenez l'Inspection économique : pointdecontact.belgique.be

Publicité trompeuse pour produit miracle



Situation

Sur Facebook, votre ami Peter vante les effets du régime « Fat/Fit » : quatre kilos perdus en une semaine !

Vous aussi, vous pouvez recevoir un échantillon gratuit.

Risque

Les offres qui apparaissent dans la colonne de droite de votre page Facebook sont des annonces publicitaires. Elles n'émanent jamais de vos amis.

Il est probable que le compte Facebook de votre ami Peter a été piraté.

En cliquant, vous signalez votre intérêt et communiquez vos coordonnées à des sociétés de marketing.

Conseil

Méfiez-vous des publicités mentionnant le nom de vos amis.

Soyez prudent : ne cliquez pas à la légère !

Tombé dans le piège ?

Informez l'Inspection économique : pointdecontact.belgique.be

Si l'on a essayé de vous extorquer de l'argent, déposez également plainte auprès de la police locale.

Offres promotionnelles accompagnées de cadeaux



Situation

Vous recevez un beau catalogue plein d'articles alléchants. Vous êtes d'autant plus tenté qu'une lettre vous promet un cadeau si vous passez commande.

Risque

La lettre qui accompagne ce catalogue n'est rien d'autre qu'une offre commerciale. Le cadeau promis est souvent de faible valeur. Le seul but est de vous inciter à acheter des produits dont vous n'avez pas nécessairement besoin.

Conseil

Ce type de démarchage n'est pas illégal.

Méfiez-vous toutefois des annonces dont le seul intérêt pour vous est le cadeau. Ce que vous devez acheter pour l'obtenir, ne risque-t-il pas de vous revenir trop cher ?

Tombé dans le piège ?

Vous ne devez rien faire car a priori, rien n'est illégal dans cette situation.

Si toutefois, vous jugez que la publicité est trompeuse ou mensongère, prévenez l'Inspection économique : pointdecontact.belgique.be

Publicité dans des annuaires professionnels



Situation

Vous recevez, au nom de votre société, une invitation à vérifier et mettre à jour les coordonnées de votre entreprise dans un annuaire professionnel.

Vous vous dites que tant qu'à faire de figurer dans cet annuaire, autant que vos données soient exactes. Un peu de publicité gratuite n'a jamais fait de tort à personne !

Risque

Avez-vous lu les petits caractères en bas de page, qui indiquent que vous vous engagez à un contrat payant dans un annuaire publicitaire pour un an ou plus ?

Conseil

Lisez toujours attentivement ce qui est écrit en petites lettres...

La publicité est rarement gratuite.

Si vous avez le moindre doute, ne signez rien !

Vous doutez de la légitimité de l'entreprise de publicité ? Vérifiez donc si elle apparaît sur la liste noire d'avertissement du SPF Economie. Veuillez toutefois noter que toutes les entreprises de publicité malhonnêtes n'y figurent pas !

Tombé dans le piège ?

Prévenez l'Inspection économique : pointdecontact.belgique.be

Time sharing : escrocs sur votre lieu de vacances

Situation

À peine arrivé à la Costa del Sol, vous sympathisez avec d'autres Belges qui vous invitent à une brève séance d'information sur un nouveau concept de vacances.

C'est sans engagement et vous y recevrez un cadeau...

Risque

C'est probablement une session de vente qui a pour but de vous vendre des vacances dans un immeuble à temps partagé (time sharing) ou d'adhérer à un club de vacances.

Ces vendeurs sont très doués : autour d'un verre et sans réel délai de réflexion, vous

risquez de signer et de prendre des engagements que vous pourriez regretter quelques heures après.

Si vous versez un acompte, il risque d'être définitivement perdu.

Conseil

Ne vous laissez pas embarquer dans ce genre de réunion.

Quoi qu'il en soit, ne signez rien et ne payez rien.

Quoi qu'on vous dise, sachez que la revente et l'échange de time sharing sont souvent très compliqués.

Tombé dans le piège ?

Déposez plainte auprès de la police (sur place et/ou en Belgique).

Informez l'Inspection économique : pointdecontact.belgique.be

Publicité trompeuse pour des voyages gratuits



Situation

Vous recevez un appel téléphonique :
« Félicitations ! Vous avez gagné un voyage d'une valeur de 1.500 euros ! Deux semaines en Turquie ! ».

Risque

Les frais de dossiers se montent à 98 euros, mais vous ne l'apprendrez que deux semaines plus tard, quand la facture arrivera dans votre boîte aux lettres.

Une fois ceux-ci versés, il y a fort à parier que vous n'entendrez plus jamais parler de votre voyage.

Conseil

Posez-vous la question : avez-vous participé à un concours ? Si ce n'est pas le cas, vous ne pouvez pas avoir gagné.

Ne payez rien et ne donnez en tout cas jamais vos coordonnées bancaires.

Tombé dans le piège ?

Déposez plainte auprès de la police locale.

Informez l'Inspection économique : pointdecontact.belgique.be

Job : promesse d'argent facile et rapidement gagné



Situation

Vous lisez une publicité sur un site web ou sur les réseaux sociaux : gagner de l'argent rapidement en travaillant chez soi. Tout ce que vous devez faire, c'est cliquer sur des publicités et pousser un maximum de vos amis à le faire à leur tour.

Risque

Ce type d'annonce publicitaire est typique des systèmes de vente pyramidale. La vente pyramidale est un système où l'on tente de gagner de l'argent en tissant un réseau de vendeurs aussi grand que possible, alors qu'aucun produit ou presque n'est vendu.

Elle fonctionne souvent avec un système de rémunération complexe où seuls ceux au sommet de la pyramide gagnent de l'argent.

Il s'agit généralement de nouvelles « entreprises », la plupart du temps de moins de deux ans, qui disparaissent aussi vite qu'elles sont apparues.

Conseil

Prenez garde aux annonces vous promettant de gagner de l'argent rapidement. Il s'agit là d'une utopie. Il faut souvent payer des frais d'entrée élevés avant même de pouvoir prendre part au système.

Si vous ne comprenez pas le système de rémunération, faites bien attention ! Ne vous fiez pas uniquement à ce que l'entreprise laisse miroiter. Recherchez des informations sur cette « entreprise » dont l'annonce est apparue, par exemple sur Google.

S'il s'agit d'un système de vente pyramidale, fuyez ! Les systèmes pyramidaux sont interdits et donc punissables, non seulement pour les fondateurs, mais aussi pour tous ceux qui y participent.

Tombé dans le piège ?

Prévenez l'Inspection économique : pointdecontact.belgique.be

Méfiez-vous des prêteurs frauduleux !

Conseil

Ne vous laissez pas aveugler par le taux d'intérêt avantageux et les formalités réduites. Emprunter de l'argent coûte aussi de l'argent et les prêts de rêve n'existent pas.

Contrôlez d'abord de façon approfondie l'identité de votre personne de contact. Seuls les intermédiaires inscrits et les prêteurs agréés par la FSMA peuvent intervenir dans la conclusion d'un contrat de crédit.

Avez-vous été questionné sur votre situation personnelle et financière ? Les vrais professionnels du crédit le font toujours !

Ne payez jamais de frais avant la signature de votre contrat de crédit.

Situation

Vous cherchez un prêt avantageux sur internet, sans trop de formalités ou de questions ennuyeuses sur votre situation financière ? Vous avez vu une annonce sur internet ou un message sur les réseaux sociaux pour des crédits faciles ? Ou bien un prêteur ayant l'air professionnel a pris contact avec vous en ligne ? Vous n'êtes qu'à quelques clics du prêt dont vous rêviez... mais vous devez d'abord verser une somme d'argent.

Risque

Ce procédé est typique des offres de crédit frauduleuses. Avant de verser le montant de crédit promis sur votre compte, les prêteurs frauduleux vous demandent d'abord de payer certains frais. Une fois payés, ils ne vous donnent plus aucune nouvelle. Dans la plupart des cas, vous ne pouvez plus récupérer les montants que vous avez payés à l'avance.

Tombé dans le piège ?

Si vous avez payé, avertissez votre banque et faites une déclaration auprès de la police.

Informez l'Inspection économique via pointdecontact.belgique.be

Réparation en urgence ? Ne vous précipitez pas !



Situation

Vous sortez de chez vous, vous claquez la porte et zut... vos clés sont restées à l'intérieur. Vous contactez d'urgence un serrurier qui vous annonce au téléphone, un prix de 100 euros. Mais après l'intervention, il vous en réclame 450...

Risque

Tous les professionnels de la réparation d'urgence ne sont pas des escrocs ! Toutefois, sans devis écrit, vous êtes à la merci de personnes mal intentionnées qui peuvent vous réclamer des sommes astronomiques pour des travaux qui ne valent pas ce prix.

Conseil

Ne contactez pas aveuglément la première entreprise qui apparaît lors d'une recherche sur internet. Privilégiez des professionnels que vous connaissez ou dont vous avez la preuve que l'entreprise est effectivement située à proximité de chez vous.

Ne vous laissez pas appâter par des prix ridiculement bas. Ces offres sont souvent trop belles pour être vraies.

Exigez toujours une offre de prix écrite et complète avant l'intervention. Et si des travaux complémentaires sont découverts en cours de réparation, demandez-en aussi le prix par écrit, avant exécution.

Tombé dans le piège ?

Signalez la fraude sur pointdecontact.belgium.be

Revente de tickets de concert



Situation

Vous rêvez d'assister au spectacle des « Queens of the Dark Moon » mais le concert est déjà sold out. Heureusement, sur internet, vous avez trouvé un site où il y a encore moyen de racheter des places. Bon, c'est vrai... Elles sont beaucoup plus chères mais pour les « Queens of the Dark Moon », vous êtes prêt à casser votre tirelire...

Risque

En Belgique, la revente de billets de spectacle à un prix supérieur à celui fixé par l'organisateur est interdite. Acheter vos billets auprès d'un revendeur non officiel, c'est risquer qu'on vous refuse l'accès au spectacle, alors même que vous avez acheté votre billet en toute bonne foi... et à prix d'or, qui plus est !

Conseil

Achetez vos billets uniquement auprès du revendeur officiel.

Évitez donc les sites internet de revente de billets de spectacle ! Ce sont souvent des sites étrangers qui ne sont pas soumis à la législation belge ! Leur activité est légale mais uniquement dans leur pays !

Ne vous fiez pas à une adresse internet « .be » : ce n'est pas nécessairement un site belge ; vous n'êtes pas forcément protégé.

Tombé dans le piège ?

Prévenez l'Inspection économique : pointdecontact.belgique.be

Cadeau à payer, vente forcée !



Situation

Aujourd'hui, au courrier, vous avez reçu un colis contenant un superbe bouquin. Vous vous dites qu'il doit s'agir d'une erreur car vous n'avez jamais commandé ce livre ! Et pourtant, la facture est bien établie à votre nom...

Risque

C'est une technique de vente forcée : le vendeur essaie de vous vendre un livre que vous n'aviez pas commandé.

Parfois même, c'est le premier numéro d'une collection par abonnement.

Conseil

Même si le montant de la facture n'est pas élevé, ne payez pas !

Pas besoin non plus de renvoyer l'article à son expéditeur, même s'il l'exige ou vous menace de poursuites en cas de non-paiement...

Personne ne peut vous condamner à payer un objet ou un service que vous n'avez jamais commandé.

Si le livre vous plaît, rangez le tout simplement dans votre bibliothèque !

Tombé dans le piège ?

Prévenez l'Inspection économique : pointdecontact.belgique.be

Location bidon : attention !



Situation

Vous cherchez un appartement à louer. Vous repérez une annonce intéressante et vous contactez la personne qui a placé l'annonce pour planifier une visite. Cette personne vous demande de verser un acompte pour vous réserver le logement.

Risque

Acceptez de payer avant même d'avoir visité le bien à louer et vous ne reverrez jamais votre argent.

Soyez prudent : il arrive même que des escrocs vous fassent visiter un bien dont ils ne sont pas propriétaires !

Conseil

Ne payez jamais rien avant d'avoir visité le bien à louer. Idéalement, mais ce n'est pas toujours possible, essayez même de ne rien payer avant d'avoir les clés en mains : ni acompte, ni garantie locative !

Une garantie locative doit obligatoirement être placée sur un compte bancaire bloqué à votre nom. Ne la versez pas avant d'avoir signé un contrat de bail.

Tombé dans le piège ?

Déposez plainte auprès de la police locale.

Signalez la fraude sur pointdecontact.belgique.be

Vente de meubles en commerce éphémère : des réductions si vous passez en magasin



Situation

On vous appelle par téléphone pour vous inviter à visiter un magasin de meubles.

On vous promet un cadeau, voire plusieurs, si vous venez en couple. Vous acceptez l'invitation.

Lors de votre visite, d'importantes réductions vous sont promises si vous achetez le jour même.

Risque

Cette technique vise à vous attirer dans un magasin où vous ne seriez pas venu spontanément et à vous faire acheter des objets dont vous n'avez pas forcément besoin.

Les prix des meubles sont surévalués, mais les vendeurs sont très bien exercés : il est très difficile de résister à leur argumentaire et aux ristournes qu'ils proposent.

Sans délai de réflexion, vous ne pouvez pas comparer avec les produits et les prix des concurrents.

Conseil

Si vous recevez ce genre d'appel, raccrochez au plus vite ! N'acceptez pas l'invitation.

Si, toutefois, vous étiez intéressé par l'acquisition de meubles, n'achetez pas sans avoir comparé avec les produits et les prix proposés par d'autres magasins.

Même si le patron entre en scène pour vous offrir des ristournes encore plus importantes, dites-vous bien que c'est dans le but de vous forcer la main.

Tombé dans le piège ?

Prévenez l'Inspection économique : pointdecontact.belgique.be

Déstockage à bas coût ne vaut **pas toujours** le coup



Situation

Un individu soigneusement habillé sonne à votre porte. Il vous explique qu'il est représentant et qu'après une foire il lui reste encore un certain nombre d'articles qu'il veut déstocker à bas prix.

Risque

Cette pratique relève souvent d'une tentative d'escroquerie. En effet, ce type de vente est rarement déclaré.

En outre, vous ne bénéficiez d'aucune garantie sur les produits achetés de la sorte.

Conseil

Pour vérifier si le vendeur est de bonne foi, demandez-lui un devis. S'il refuse, ne signez rien et n'achetez rien.

Dans tous les cas, accordez-vous un délai de réflexion.

Vérifiez et comparez avec les prix de la concurrence.

Tombé dans le piège ?

Déposez plainte auprès de la police locale.

Informez l'Inspection économique : pointdecontact.belgique.be

Un entrepreneur trop entreprenant...



Situation

Un entrepreneur sonne à votre porte. Il vous propose ses services pour rafraîchir la toiture ou ramoner vos cheminées.

Risque

Un entrepreneur sérieux ne procède pas de la sorte. Il y a fort à parier que le travail presté ne sera pas déclaré (travail au noir). Dans ce cas, vous êtes responsable en cas d'accident et vous n'avez aucun moyen de recours si les travaux sont de mauvaise qualité.

Conseil

Accordez-vous un délai de réflexion.

Vérifiez si cette personne est un véritable indépendant.

Pour vérifier si l'entrepreneur est de bonne foi, demandez lui un devis. S'il refuse, ne signez rien, ne commandez rien et ne lui payez rien.

Tombé dans le piège ?

Déposez plainte auprès de la police locale.

Informez l'Inspection économique : pointdecontact.belgique.be