

!! Arnaques sur Internet !!

Soyez sur vos gardes, ils sont partout !

Les scénarios (adaptables à la majorité des arnaques dites à la nigérianes)

- [Le principe de base](#)
- [Les terrains de chasse](#)
- [Les pièges les plus courants](#)
 - [Dons, ventes, achats d'objets, d'animaux, locations saisonnières...](#)
 - [Prestations \(fêtes, cérémonies, mariage...\)](#)
 - [Offres d'emploi](#)
 - [Sites de rencontres](#)
 - [Cyber-chantage](#)
 - [Loteries](#)
 - [Offres de prêt ou de bourses d'études](#)
- [Les signaux d'alerte](#)
- [Les modes de paiement à éviter](#)
- [En cas de doute](#)
- [Signaler un comportement ou contenu suspect](#)
 - [Informez et témoignez](#)
 - [Signalez aux autorités compétentes](#)
- [Déposer une plainte](#)
- [Autres lien utiles](#)

Le principe de base

Le principe de base de ces arnaques, appelées également [scam](#) ("ruse" en anglais), est de vous convaincre de faire un transfert d'argent en utilisant généralement les services Western Union ou autres modes de paiements, par ailleurs interdits, dans ce type de transaction.

En effet, contrairement à ce qu'affirment les escrocs, ils encaissent sans difficulté les fonds sans avoir besoin ni de code secret ni de justification d'identité. Dans certains pays et compte tenu que certains agents font partie des réseaux, il leur suffit de connaître le nom de l'expéditeur

Les terrains de chasse

Ils vous contactent par email, sur les sites de rencontres, les réseaux sociaux et sur les sites de petites annonces. Dans ce dernier cas, ils vous vendront ou vous achèteront n'importe quoi en se faisant passer, soit pour des vendeurs, soit pour des acheteurs, soit pour des loueurs de biens immobiliers, organisateurs d'évènements, employeurs... Suivant les scénarii qu'ils utilisent, ils n'hésitent pas à créer des sites frauduleux pour vous convaincre de leur bonne foi (sites de transporteurs, de banques, d'associations caritatives...). Dans ce dernier cas, les escrocs utilisent parfois la technique du phishing c'est à dire qu'ils imitent un courrier officiel d'une banque, d'un marchand en ligne (par exemple eBay) ou d'un organisme de paiement (PayPal), qui vous demande de confirmer vos informations personnelles... qu'ils récupèrent.

Les pièges les plus courant

Dons, ventes, achats d'objets, d'animaux, locations saisonnières...

Dans le rôle de l'acheteur :

Il exige des copies de différents documents officiels (carte d'identité, certificat de non gage, carte grise etc.) qui lui serviront à usurper votre identité lors de ses futures arnaques.

Il vous persuade, à l'aide de faux intervenants (transporteurs, douaniers...) que vous devez verser des frais pour encaisser son paiement, frais qu'il vous promet d'inclure dans son paiement afin de vous rembourser. Il peut également vous faire parvenir une fausse confirmation bancaire, ou un chèque faux ou falsifié dont le montant est supérieur à la somme convenue : il exige donc le remboursement rapide du trop perçu par mandat international. Concernant les chèques falsifiés, la banque met parfois plusieurs jours à s'apercevoir de la supercherie. Votre compte est donc crédité pendant quelques jours mais sera invariablement re-débité.

Dans le rôle du vendeur (ou généreux donateur) :

Il copie une annonce réelle, textes et photos mais propose un prix attractif afin d'attirer le maximum de d'acheteurs. Ensuite, il utilise à peu près les mêmes techniques que lorsqu'il jouait l'acheteur : frais douaniers, intervenants divers (banques, transporteurs, douaniers) pour vous convaincre que l'article que vous achetez est en transit, prêt à vous être livré.

Malheureusement pour vous, il y a des contretemps et donc des frais supplémentaires à payer qu'il vous propose de déduire du prix convenu.

Prestations (fêtes, cérémonies, mariage...)

Cette arnaque concerne musiciens, photographes, compagnies de théâtre... L'arnaqueur vous contacte pour que vous veniez animer un évènement à l'étranger. Il vous remboursera tous les frais mais vous devez avancer le prix des billets. Il est très "sympa" et vous dirige vers le site d'une fausse agence de voyage sur lequel vous obtiendrez les meilleurs prix.

Offres d'emploi

Dans ce type d'escroquerie, la plus répandue est actuellement celle de "consignataire". Le travail consiste à réacheminer des colis.

Pour établir votre contrat de travail, il vous demande des copies de documents officiels. Il vous envoie ensuite un contrat de travail bidon et commence à passer des commandes à votre nom en payant avec un n° de CB obtenu par phishing. Vous recevez ces colis et les réacheminez, comme prévu dans votre contrat. En fin de mois, lorsque vous réclamez votre salaire, il vous informe que vous devez payer des frais pour pouvoir encaisser la somme. Vous faites un transfert et le salaire n'arrive jamais. Quelques semaines plus tard, vous commencez à recevoir les relances de paiements de fournisseurs escroqués et vous avez beaucoup d'ennuis...

Une autre variante consiste à vous faire signer un contrat avec une agence de publicité qui vous annonce que vos photos (trouvées sur le net) ont été sélectionnées pour participer à une campagne d'affiches publicitaires. Pour votre rémunération, on vous enverra alors de faux chèques ou de faux traveller chèques. Vous retiendrez 20 % pour votre « salaire » et devez renvoyer les 80% par Western Union.

Sites de rencontres

Une personne très amoureuse de vous croule sous des tonnes de problèmes : vous êtes embarqué dans un scénario romantico/dramatique très compliqué et vous vous démenez pour sortir l'amour de votre vie de situations catastrophiques en accédant à la demande d'argent de l'escroc, toujours par Western Union : maladie d'un proche, décès, problème avec la police, billets d'avion etc. Cette escroquerie est la plus destructrice car elle met en jeu les sentiments et le moi profond. C'est un véritable viol psychologique.

Cyber-chantage

C'est un type d'escroquerie en nette recrudescence.

Après les histoires romantico-rocambolesques destinées à vous convaincre d'envoyer de l'argent par Western Union, voici le principe de cette variante (en nette recrudescence) :

1. Une discussion plus qu'amicale s'engage et l'inconnu(e) vous entraîne sur MSN et vous incite à une webcam « hot ». Il vous fait parler de votre situation familiale, de votre situation professionnelle, de vos amis... Si vous avez un compte de type facebook, tous vos contacts seront mémorisés.
2. Cette personne insiste pour avoir une discussion par webcam et vous incite à dire ou faire des "choses" intimes via la cam
3. Vous recevez ensuite des mails issus de faux policiers vous menaçant d'envoyer les images capturées sur youtube et à vos amis/collègues/familles/connaissances si vous ne payez pas une forte (pseudo)amende.

Loteries

Maître ANGE CROILLEMOA vous informe que vous avez gagné le jackpot d'une loterie à laquelle vous n'avez jamais participé. Pour encaisser la somme, vous devez d'abord payer des frais, mais vous ne verrez jamais rien.

Offres de prêt ou de bourses d'études

Mr Papa NOEL vous contacte pour vous proposer un prêt. Il vous demande quelques copies de documents officiels puis exige le paiement d'intérêts ou de frais bancaires pour pouvoir finaliser ce prêt. Il vous envoie même une preuve du virement qui est en cours !

Les signaux d'alerte

- Offre anormalement alléchante
- Faux email de PayPal demandant le remboursement par Western Union d'un trop perçu ou de frais imprévus
- Interlocuteur à l'étranger : Afrique de l'Ouest, certains pays de l'Est, Grande-Bretagne...
- Insistance pour un type de paiement déconseillé dans les transactions entres inconnus (Western Union, Moneygram, Swift... liste détaillée dans un autre paragraphe)
- Faux numéro de téléphone ou numéros commençant par 004, 00225,00229
- Accent incompatible avec la nationalité annoncée
- métiers valorisants et au-dessus tout soupçon (curé, notaire, diplomate, avocat...)
- Policiers, avocats, banquiers, douaniers, notaires etc. utilisant des adresses de messageries gratuites (ex: @hotmail, @yahoo, @laposte, @nantes, @paris etc...) ou des adresses de messageries ressemblant à des adresses professionnelles xxxxx@financier.com ou encore xxxxxx@consultant.com ([les adresses email trompeuses](#)).
- Toujours très pressés de faire la transaction
- Trop de justifications données sans raison apparente
- Réception d'un paiement supérieur à celui convenu et demande le remboursement du trop perçu.
- Intervention d'un tiers "de confiance" (transporteur, avocat, douanier, notaire...)
- Histoires dramatiques destinées à vous convaincre de faire un transfert d'argent (maladie, problème avec la justice, investissements, passeports...)
- Vous posez des questions mais il répond toujours à côté (souvent, les mails d'arnaques sont pré-formatés car la plupart de ces escrocs parlent très mal le français)
- Il vous réclame la copie de nombreux documents officiels (ce qui lui permettra d'usurper votre identité pour ses prochaines arnaques)
- vous recevez un email imitant un courrier officiel d'une banque, d'un marchand en ligne (par exemple eBay) ou d'un organisme de paiement (PayPal), qui vous demande d'aller confirmer vos informations personnelles (les banques ne contactent pas leurs clients pour leur demander de fournir des informations sensibles comme les mots de passe ou les identifiants en ligne)

* une adresse service.paypal@financier.com **n'est pas une adresse email de paypal**

* une adresse client_ebay@consultant.com **n'est pas une adresse email de E-Bay**

Dans cette exemple l'adresse aurait du être xxxxxx@paypal.fr ou xxxxxx@ebay.com

Les modes de paiement à éviter

Pour une transaction avec un inconnu, ne jamais utiliser :

Western Union, AlertPay.com, anypay.com, AuctionChex.com, BillPay.ie, Billpoint.com, ecount.com, cardserviceinternational.com, CCAvenue, ecount, e-gold, eHotPay.com, ePassporte.com, EuroGiro, FastCash.com, Google Checkout, gcash, GearPay, Goldmoney.com, graphcard.com, greenzap.com, ikobo.com, Liberty Dollars, Moneygram.com, neteller.com, Netpay.com, paychest.com, Payko.com, payingfast.com, paypay, Postepay, Qchex.com, rupay.com, sendmoneyorder.com, stamps, Stormpay, wmtransfer.com, xcoin.com, le service mandat cash de la poste.

En cas de doute

La première chose à faire est de laisser tomber. Si vous souhaitez malgré tout poursuivre :

- refusez toute vente ou achat payé via Western Union, Moneygram...
- faites une [recherche sur Google](#) avec les noms utilisés, les emails utilisés, des fragments de phrases pour voir s'il existe des similitudes avec d'autres arnaques
- consultez [la liste des sites frauduleux sur aa419.org](#).
- faites une recherche sur [hoaxbuster.com](#) et sur <http://www.croque-escrocs.fr>

Signaler un comportement ou contenu suspect

Informez et témoignez

La première chose à faire est d'informer le maximum d'internautes afin que les plus prudents trouvent votre témoignage s'ils font une recherche.

Donc, copiez sur <http://www.avenfrance.org/forum/> :

- les emails reçus (en prenant soin d'enlever vos infos personnelles)
- les adresses email utilisées par les escrocs
- s'il s'agit d'une petite annonce, ajoutez l'adresse du site sur lequel vous avez trouvé cette annonce (avec si possible, les références de l'annonce)

Signalez aux autorités compétentes

Pour la Belgique : <https://www.ecops.be/webforms/Default.aspx?Lang=FR>



The screenshot shows the eCops website interface. At the top, there is an orange header with the eCops logo and navigation links for Nederlands, Français, Deutsch, and English. Below the header, the text reads "Bienvenue" and provides information about the service: "eCops est un point de contact en ligne où vous pouvez, en tant qu'utilisateur d'Internet, signaler des délits commis sur ou via l'Internet." It lists several types of incidents that can be reported, such as receiving unsolicited emails or seeing suspicious content. A "Signaler" button is prominently displayed. At the bottom, there are logos for the Police and Economie, along with a disclaimer and contact information.

Pour la France : <https://www.internet-signalement.gouv.fr/>



The graphic consists of two main sections. The top section is a dark blue rectangle with white text that reads "INFO ESCROQUERIES" at the top, followed by the phone number "0811 02 02 17" in large font, and "COÛT D'UN APPEL LOCAL" below it. The bottom section is a red rectangle with white text that reads "POUR SIGNALER UN COURRIEL OU UN SITE INTERNET D'ESCOQUERIES" and the website address "www.internet-signalement.gouv.fr".

Déposer une plainte

Si vous avez subi un préjudice, **n'hésitez pas à le faire**. Attention, aucun policier ou gendarme, ne peut refuser une plainte sans s'exposer à des sanctions (article 15-3 du code de procédure pénale)
Les escrocs vont utiliser votre identité pour continuer leur activité.

La plainte permet de prouver votre bonne foi, de faire reconnaître votre statut de victime et de permettre d'alerter la justice et les pouvoirs publics sur ce phénomène

Déplacez-vous au commissariat ou à la gendarmerie la plus proche en vous munissant de tous les renseignements en votre possession :

- références du ou des transferts d'argent effectués,
- références de la ou des personnes contactées : adresse de messagerie ou postale, pseudos utilisés, numéros de téléphone, fax, copie des courriels/courriers échangés...,
- tout autre renseignement pouvant aider à l'identification de l'escroc.

Si vous habitez Paris :

BEFTI (Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information)

163 avenue d'Italie

75 013 Paris

Tél. : 01 40 79 67 50

Si vous habitez en région :

Portez plainte au Service Régional de Police Judiciaire de votre localité (Gendarmerie ou Police Nationale).

Renseignez-vous pour savoir si ce service dispose d'un enquêteur spécialisé criminalité informatique (ECSI) qui sera plus compétent pour prendre votre plainte.

Autres lien

- OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication)
- Les signaux d'alarme pour les acheteurs (Ebay)
- Campagne d'information sur la lutte contre les escroqueries (Ministère de l'Intérieur, de l'Outre-Mer et des Collectivités Territoriales).
- Alerte aux arnaques (Ambassade de France en Côte d'Ivoire)
- Pétition exigeant des mesures préventives.
(initiée par AVEN Europe)