

Il y a encore un nombre infini de formes d'escroquerie et parfois elles sont difficiles à déceler. Ci-dessous, vous trouverez quelques trucs afin de mieux vous en protéger.

QUELQUES TRUCS

Général

- Protégez votre ordinateur par des mises à jour régulières de votre système d'exploitation (généralement Windows) et utilisez toujours la dernière version de votre programme anti-virus.
- Utilisez uniquement des logiciels d'origine et mettez-les à jour.
- N'ouvrez pas de mails de personnes que vous ne connaissez pas, et ne cliquez surtout pas sur les liens de ces mails. Ils peuvent cacher des virus de toutes sortes et infecter insidieusement votre ordinateur.
- Les banques et les entreprises publiques ne vous contacteront jamais par mail pour vous demander vos données personnelles. Effacez immédiatement tous les mails qui vous le demandent. Si vous doutez, prenez contact avec l'institution en question.
- Contrôlez le nom, adresse, numéro de téléphone, adresse mail du vendeur/acheteur ou de la personne inconnue qui vous offre de l'argent via mail en les recherchant dans des moteurs de recherche sur Internet (par exemple Google). Les escrocs ressortent souvent vu que d'autres victimes racontent leur histoire sur l'un ou l'autre forum.
- Ne payez JAMAIS via des systèmes de transfert d'argent du type Western Union ou Moneygram à un inconnu. Ce sont de bons systèmes pour envoyer rapidement de l'argent à des personnes que vous **CONNAISSEZ**. Mais ne l'acceptez pas comme moyen de paiement quand vous ne connaissez pas l'acheteur ou le vendeur en question. Cette règle d'or vaut pour tous les types d'escroqueries (sites d'enchères, faux héritages, loteries, etc.).



Acheter et vendre sur des sites d'enchères / petites annonces

- Ne faites d'achats que lorsque vous avez reçu assez de garanties que le vendeur ou l'acheteur est sérieux. Regardez par exemple sur le site d'enchère le feedback du vendeur/acheteur. Le système de feedback n'est pas étanche, mais vous donne quand même une indication. Regardez aussi depuis quand il ou elle est membre. S'il /elle est membre depuis longtemps, il y a plus de chance que ce soit un acheteur/vendeur honnête.
- Lorsqu'un article ou un bien est vendu à un prix bien plus bas (par exemple une belle Ferrari pour quelques milliers d'euros), soyez très prudent. Il y a beaucoup de chance que le vendeur ne possède pas l'auto et que ce soit une escroquerie.
- Ne donnez jamais d'acompte sans avoir vu vous-même l'objet. S'il se trouve à l'étranger, allez alors l'examiner, ou cherchez un autre bien ou article dans votre pays.
- Si vous recevez un chèque de l'acheteur, ne faites rien avant que votre banque ne vous ait confirmé qu'il s'agit bien d'un vrai chèque et qu'il est bien couvert. Cela peut durer quelques semaines. Dans l'attente, n'envoyez pas d'argent en retour à l'acheteur (s'il a fait un chèque d'un montant plus élevé) et attendez avant d'envoyer la marchandise.

Fausse loterie/héritage

- Vous ne pouvez jamais gagner à une loterie à laquelle vous n'avez pas participé. Ignorez tous les messages qui vous promettent beaucoup d'argent.
- Cela vaut également pour les faux héritages: comment le fils d'un défunt président africain peut-il vous joindre ? Parce qu'il a envoyé un mail spam à un million de personnes en même temps. Escroquerie pure!
- Ne prenez pas de rendez-vous avec les escrocs, vous risqueriez non seulement de perdre encore plus d'argent, mais aussi des menaces physiques.

Fraude à l'émotion

- Envoyez de l'argent aux bonnes œuvres que vous connaissez. Si vous êtes contacté par mail par une organisation d'aide connue et que vous voulez contribuer, contrôlez les données bancaires sur le site web de l'organisation en question.
- Restez sur vos gardes lorsqu'un candidat-partenaire commence à demander de l'argent.
- Travaillez avec une agence de rencontre reconnue ou contrôlez le nom du site de rencontre et les données de votre candidat-partenaire sur Internet en les recherchant dans un moteur de recherche (comme Google).
- Ne partez pas directement du principe que l'expéditeur d'un message via email est réellement la personne que vous connaissez (ami, famille,..). Il existe d'innombrables manières de se faire passer pour quelqu'un d'autre via mail.
- Lorsque vous recevez un message de détresse d'une personne que vous connaissez: contactez la personne en question, son compte mail a probablement été piraté. Mettez-le au courant afin qu'il puisse entreprendre les démarches nécessaires afin de reprendre son compte et avertir ses adresses de contact de l'escroquerie.

Vous pourrez trouver encore d'autres conseils sur les sites web suivants :

economie.fgov.be
www.cecbelgique.be
www.web4me.be
www.saferinternet.be
www.fedpol.be (Surfons tranquilles, fraude internet)
www.westernunion.be

Infractions constatées sur Internet? Les signalements peuvent être faits via

www.ecops.be.

Victime? Déposez plainte auprès de votre service de police locale

Fraude via internet

Depuis l'apparition d'Internet, les escrocs ont trouvé de nouvelles manières de soutirer facilement et rapidement de l'argent à beaucoup de personnes. Aujourd'hui, une grande partie de la population communique par mail et a, soit à la maison, soit au travail, un accès à internet. La chance que vous soyez un jour ou l'autre confronté à des personnes qui essaient de vous escroquer par cette voie est donc bien réelle. Soyez donc toujours attentif lorsque des **INCONNUS** tentent de vous approcher via Internet.

Actuellement, il est difficile d'échapper à la multitude de **SPAM** qui sont envoyés dans nos boîtes mail. Entre tous ces messages publicitaires indésirables de personnes ou d'entreprises dont on n'a encore jamais entendu parler, se trouvent souvent des emails – en anglais ou dans un mauvais français ou néerlandais – qui ont comme sujets les loteries, la succession d'un chef d'Etat africain, de l'aide par des transactions financières, des investissements exotiques ou autres.



Les escrocs sont très créatifs et cherchent toujours de nouvelles manières de soutirer de l'argent aux gens. Pourtant, nous retrouvons toujours les mêmes méthodes; ci-dessous vous trouverez les plus courantes. Le meilleur conseil: **IGNOREZ CES MAILS ET EFFACEZ-LES SANS ATTENDRE**. N'y prêtez surtout pas attention, sinon, vous risquez de perdre beaucoup d'argent!

Ainsi, vous gagnez par exemple tout à coup quelques millions de dollars ou d'euros, et ce, bien que vous n'ayez jamais participé à aucune **LOTERIE**. Pour recevoir l'argent, vous devez d'abord payer toutes sortes de frais: frais administratifs, frais de notaire, frais de banque, etc... Ou bien la veuve d'un défunt chef d'Etat Africain vous écrit personnellement – quel honneur ! – pour vous demander de l'aider à transférer **L'HERITAGE** qu'elle a reçu de son mari hors du pays par des voies détournées. La seule chose que vous devez faire est simplement d'avancer quelques montants et plus tard, vous recevrez un pourcentage garanti du montant total qui se chiffre naturellement en millions.

Il existe beaucoup de variantes de cette forme d'escroquerie, mais le principe de base reste le même: vous devez avancer de l'argent à un inconnu pour récolter une somme d'argent promise. Les escrocs font souvent usage de documents ayant l'air vrai (de notaires, banques, passeports, ...) qu'ils envoient par mail. Ceux-ci sont des faux! Beaucoup de ces mails sont aussi soi-disant de votre **BANQUE**, qui vous contacte parce qu'il y a des problèmes avec leur système de paiement via Internet, ou parce que vos données doivent être mises à jour. Pour ce faire, vous devez cliquer sur un hyperlien dans le mail, et celui-ci semble vous amener vers la page de la banque où on vous demande de donner vos login et mot de passe, et parfois même d'autres données personnelles, telles que votre adresse, numéro de téléphone et date de naissance («*phishing*»). Ne le faites surtout pas! Les escrocs essaient de cette manière de vous voler vos données personnelles afin d'en abuser plus tard. N'oubliez pas que votre banque ne vous contactera **JAMAIS** par mail pour vous demander vos données personnelles!



Fréquemment, il y a aussi les escroqueries via les **SITES DE PETITES ANNONCES**, tel que Ebay, Autoscout24, 2dmain, etc... Si vous respectez quelques règles de base et que vous faites preuve d'une bonne dose de prudence, faire des achats sur Internet ne doit pas vous effrayer.

Les escrocs jouent aussi de plus en plus souvent avec les **SENTIMENTS** dans leur tentative de soutirer de l'argent. Vous recevez des messages déchirants sur des **CATASTROPHES NATURELLES** ou des enfants gravement malades dans lesquels on vous demande de verser une contribution généreuse à une organisation inconnue. Ces **ANIMAUX** qu'on offre gratuitement – le propriétaire ne peut plus s'en occuper - pour lesquels vous n'aurez qu'à payer les frais de transport.

Un nouvel **AMOUR** ou **AMI** que vous avez rencontré par Internet, et qui vous demande d'envoyer de l'argent pour de nouveaux vêtements, le billet d'avion vers la Belgique, leur passeport, ...

Ou une **PERSONNE QUE VOUS CONNAISSEZ** (membre de la famille, ami, connaissance..) vous envoie un **MESSAGE DE DETRESSE** dans lequel il vous demande de l'argent: il est à l'étranger et a été attaqué. Ou il a perdu son portefeuille. Ou est impliqué dans un accident de la route... Ou.. Vous êtes le seul qui puisse l'aider! L'intéressé est en réalité simplement chez lui et n'est pas au courant de ce message envoyé: son compte mail a subi un hacking et les escrocs ont envoyé le même message à tout son carnet d'adresses.

Gardez la tête froide car, au final, vous vous retrouverez souvent les mains vides

