Les arnaques, protégez-vous !

Protégez-vous des arnaques du web !

Lorsqu'il s'agit de trouver un bon plan pour gagner de l'argent, les escrocs et les arnaques Internet ne manquent pas.

Des gens sont prêts à vous vendre n'importe quoi en jurant sur leur honneur que ça marche. Leur but ? Se faire de l'argent sur votre dos. La morale ? Ils n'en ont pas vraiment. Ils arrivent à dormir la nuit ? Oui, très probablement, et c'est ça le pire.

J'aime différencier les arnaques sur Internet (et les escrocs) selon plusieurs types ; bien que comme vous le constaterez par vous-même, ces catégories se recoupent largement.

Attention : j'utilise le mot arnaque partout, même si parfois, ce n'est pas vraiment une arnaque, mais plutôt un raccourci qui consiste à mettre sous silence quelques détails.

L'arnaque de l'investissement : Donnez-moi votre argent !

C'est l'arnaque la plus courante.

Pour commencer à gagner de l'argent, vous devez d'abord **acquérir un kit de démarrage ou un ebook** ; tout y est expliqué. Vous devez donc débourser de l'argent avant de commencer. Et vous rentrerez rarement dans vos frais.

C'est également comme ça que les régies à revenus partagés fonctionnent, comme Profits25 : on vous demande d'abord de verser 50 euros qui soi-disant vont se transformer ensuite en 70 euros…

L'arnaque de l'argent sur le net : Vous gagnerez gros !

On vous fait croire que vous gagnerez beaucoup d'argent, mais ce n'est pas le cas. Lire des mails ou répondre à des sondages rémunérés ne vous rapportera jamais plus que 100 euros par mois, contrairement à ce que certains vous inciteront à penser.

L'escroc quant à lui aura empoché une commission grâce à votre inscription ou vos clics.

L'arnaque de la fiabilité : C'est 100 % fiable et 0 % arnaque !

On vous dira que ce placement en bourse ne court **aucun risque**. Ou que ce système est **mathématiquement prouvé** et qu'il gagne à tous les coups.

Mais où sont les preuves ?
Un placement en bourse n'est jamais sans risque. Et un système qui gagne à tous les coups aura probablement été décelé et interdit.

L'arnaque du temps : Vous gagnerez rapidement beaucoup d'argent !

Ce type d'arnaque Internet est beaucoup plus subtil et difficile à déceler au préalable. Ce n'est pas basé sur le mensonge en tant que tel, mais plutôt sur une omission de certains détails.
L'escroc omettra de vous dire que la technique qu'il vous propose va vous demander **beaucoup de temps** pour commencer à vous rapporter de l'argent.
Par exemple, on vous incitera à faire de la mise sous pli en vous faisant croire que vous gagnerez un SMIC par mois. Pourtant, la vérité est que ça demande du temps, beaucoup de temps. Vous n'avez certes pas dépensé un centime, mais **les gains tarderont à venir** – et ça, certains n'hésitent pas à vous le cacher.

L'arnaque de la facilité : Vous n'avez besoin d'aucune connaissance particulière !

Ici, il s'agit de vous faire croire que vous pourrez gagner de l'argent **sans connaissances particulières**. N'importe qui pourra gagner un salaire extra voire devenir riche en s'abonnant à tel service ou en achetant tel produit.
Vous n'avez effectivement pas besoin d'aptitudes ou de talents *au préalable*, mais le problème c'est que vous devrez apprendre de nouvelles choses pour commencer à gagner *vraiment* de l'argent.
Par exemple, monter un blog est à la portée de tout le monde, mais vous serez forcés d'acquérir de **solides connaissances** en référencement, marketing, écriture…

L'arnaque de l'expertise : Je suis un expert, suivez-moi !

Certains se présentent comme de véritables experts dans leurs domaines, et vont vous inciter à coup de **fausses preuves et faux témoignages** à souscrire à leurs services.
C'est le cas de ces anciens soi-disant traders, ou de ces blogueurs qui vendent des ebooks expliquant comment ils vivent de leurs blogs (cherchez l'erreur : ils vivent de leurs blogs en vendant un ebook qui explique comment vivre de son blog.)

L'arnaque de l'ignorance : Vous ne trouverez pas cella ailleurs !

Vous n'avez pas les connaissances ou l'expérience nécessaires dans un domaine pour savoir que l'offre qui vous est faite est **disponible gratuitement**, et c'est tant mieux pour l'escroc.
Par exemple, un arnaqueur très connu sur Internet vend une formation à 1000 euros pour vous aider à créer votre blog et lancer votre affaire. Oui, mille euros. Sachant que 95 % des informations données dans cette formation sont disponibles gratuitement.

L’arnaque de l’argent passif : Ce sont des revenus automatisés !

On vous fait croire que la méthode en question est automatisée et que vous n’aurez presque rien à faire, sauf vous asseoir dans votre fauteuil et voir **défiler l’argent**.

Il existe effectivement des moyens de gagner de l’argent de manière automatisée, mais c’est au prix de **beaucoup de temps, de travail et d’argent**. Un musicien gagne de l’argent sur les droits d’auteur chaque fois que l’un de ses titres est joué à la radio : c’est de l’argent automatisé, mais il a dû fournir de nombreux efforts pour en arriver là.

Méfiez-vous !

Quand on vous propose un bon plan pour gagner de l’argent, faites attention et assurez-vous que cette opportunité n’utilise pas en fait l’un des types d’arnaques décrits ci-dessus.

Il y a encore trop de gens qui se font avoir.

Tant que nous serons sur Terre, certains de nos semblables essaieront de nous soutirer de l’argent par n’importe quel moyen. Certains disent que c’est la nature humaine.

* Pour ma part, je préfère vous dire la vérité, vous avertir sur les **arnaques Internet**, et vous proposer plein de manières de gagner de l’argent. Des manières prouvées et sans arnaque.

** (Je plaisante bien-sûr !)*

Conseils pour éviter les arnaques aux sentiments (Site de rencontre)

1 – L’une des premières choses à demander à une personne qui s’intéresse à vous, c’est de savoir DANS QUELLE RÉGION, VILLE OU VILLAGE ELLE HABITE. Sans forcément lui demander son adresse exacte. La personne doit pouvoir être physiquement accessible. Si elle ne l’est pas pour vous, faites-le lui savoir. Vous pouvez très bien être accessible pour lui / elle.

Privilégiez les contacts de proximité

2 – Peu importe si la personne à l’autre bout reste sur le site de rencontre ou vous en fait sortir en vous donnant rendez-vous sur WhatsApp, Hangouts ou Skype. De toute façon, il faudra bien « sortir » tôt ou tard du site de rencontre. Ceci dans le but de faire une rencontre pour de vrai. Mais un de mes conseils est qu’il faut absolument le / la contacter en communication vidéo en direct au moins 1 fois EN DEHORS DU SITE DE RENCONTRE. Ceci pour s’assurer ainsi qu’il ne s’agit pas d’une hôtesse payée par le site de rencontre. Mais également pour vérifier que votre partenaire correspond bien à son profil.

Si elle ne peut pas à cause, selon elle, de sous-équipement ou de panne et qu’elle ne fait rien pour y remédier, passez votre chemin. De plus, il faut faire attention avec Skype. Car Skype permet d’envoyer une vidéo en faisant croire qu’il s’agit d’un direct. Cela permet à l’escroc de passer une fausse vidéo sur l’écran de son ordinateur. Et donc de vous l’envoyer en la faisant passer pour une vraie communication en direct. Il faut donc faire particulièrement attention qu’il y a bien interaction entre vous et votre partenaire. Il faut que cela soit bien du direct.

Ne pas céder aux demandes d'argent

3 – Lorsque vous devez vous déplacer pour vous rencontrer pour de vrai, il faut absolument, quel que soit la distance qui vous sépare, que la personne qui se déplace paye son déplacement ou son voyage. Quitte à ce qu'une fois que vous vous voyez pour de vrai, vous lui offriez une soirée au cinéma, au restaurant, un voyage à deux, etc.

Tant que vous êtes ensembles PHYSIQUEMENT, pas de problème. Par exemple, si votre partenaire vous dit qu'elle aimerait bien venir vous voir mais qu'elle vous demande de l'aider, proposez-lui d'aller la voir vous, au lieu de lui envoyer de l'argent pour qu'elle vienne. Si vous ne pouvez pas vous vous rencontrer pour de vrai à cause d'une trop grande distance (ou à cause de n'importe quelle autre raison), c'est qu'il s'agit d'une histoire d'amour dite impossible. Vous perdez donc votre temps.

4 – Un des autres conseils important, votre partenaire ne vous doit JAMAIS vous demander de l'argent. Même si vous avez pu avoir une communication vidéo en direct. En effet, même si la personne à l'autre bout correspond à son profil, cela ne l'empêche pas de vous arnaquer aux sentiments.

Si elle vous demande de l'aide, offrez-lui dans la mesure du possible de l'aide en nature, JAMAIS en espèces. Comme par exemple un billet d'avion est toujours nominatif, il est impossible à l'escroc de le revendre. Moi, par exemple, je n'aide financièrement que ma compagne, je n'aide financièrement PERSONNE D'AUTRE.

Gardez en tête que le but des sites de rencontres est de faire… des rencontres

5 – Le site de rencontre ou le logiciel de tchat sur lequel vous vous rencontrez doit pouvoir vous permettre de garder les historiques de conversations, IMPORTANT. Je connais un certain logiciel de rencontre qui efface tous les historiques de conversations lorsque vous le quittez. Avoir l'historique vous permettra de mettre en évidence certaines incohérences dans le discours de votre contact. Et éventuellement de démasquer un arnaqueur.

6 – Ne perdez jamais de vue qu'il s'agit de faire des rencontres RÉELLES que cela soit une rencontre sexy ou romantique. Ce qui veut dire que la relation DOIT évoluer dans ce sens. Et ceci dans un délai raisonnable en fonction de la distance qui vous sépare ☺. Une relation qui s'éternise sur internet peut être le signe d'une relation qui n'a aucune vocation à devenir réelle. Comme celle qu'un escroc peut entretenir dans le but de soutirer de l'argent.

7 – Une grande différence d'âge est toujours possible en terme de relation amoureuse. Mais si vous êtes abordé par un contact nettement plus âgé ou nettement plus jeune, alors les possibilités qu'il s'agisse d'une arnaque augmentent. Soit la personne plus âgée peut vous arnaquer en profitant justement de son plus grand recul sur la vie. Soit la personne plus jeune peut être un leurre, juste une photo avec un arnaqueur derrière.

Arnaques sur Internet ! Détecter les e-mails malveillants

L'e-mail reste l'un des outils les plus prisés des pirates sur Internet. Voici quelques conseils pour repérer les messages malveillants et ne pas être victime de tentatives de phishing.

Un e-mail malveillant est un message électronique frauduleux qui a pour but d'inciter le destinataire à effectuer un transfert de fonds ou à se rendre sur un site frauduleux où lui seront demandés ses identifiants, ses mots de passe ou ses données bancaires. C'est la technique de l'hameçonnage, ou **phishing** en anglais. Il peut aussi être invité à ouvrir une pièce jointe dans laquelle se cache un programme capable de voler des données présentes sur l'ordinateur.

LES INDICES QUI DOIVENT VOUS ALERTER

La présentation

Ne vous faites pas abuser par la présence de logos officiels, de liens vers des sites connus ou d'informations vous concernant. La présence de fautes d'orthographe ou de grammaire doit aussi vous mettre la puce à l'oreille.

L'expéditeur

Les pirates n'hésitent pas à se faire passer pour une banque, une administration (Caf, service des impôts…), une entreprise (EDF, Orange…) voire une personne de votre connaissance pour gagner votre confiance.

Le message

Il joue le plus souvent sur l'empathie (une personne a besoin d'aide), l'urgence (votre électricité sera coupée si vous ne réagissez pas vite), la peur (vous risquez d'être poursuivi si vous ne payez pas) ou fait miroiter une promesse d'argent ou un remboursement.

Le lien hypertexte

Vérifiez que l'adresse du site officiel vers laquelle il est censé renvoyer soit la bonne (www.microsoft.com et pas www.security-microsoft.com ou www.micosoft.com par exemple).

LES BONS RÉFLEXES

- Ne répondez pas au message, ne cliquez sur aucun lien y compris celui censé permettre de se désabonner, n'ouvrez pas de pièce jointe et ne remplissez aucun formulaire.
- Faites preuve de bon sens : aucun organisme ne vous demandera par e-mail de lui communiquer des informations personnelles.
- En cas de doute, contactez l'organisme censé vous avoir envoyé l'e-mail par téléphone ou en passant par la page d'accueil de son site Internet et non par le lien proposé dans l'e-mail.
- Signalez l'e-mail sur la plateforme gouvernementale Internet-signalement.gouv.fr.
- Supprimez-le et videz la corbeille.
- Pour une protection au quotidien, certains éditeurs d'antivirus proposent des suites complètes comprenant diverses fonctions protectrices, dont l'antiphishing.

Les arnaques les plus courantes sur Internet que vous pouvez repérer, notamment certaines qui sont plutôt visibles. Comment éviter les arnaques sur Internet et comment identifier qu'il s'agit d'une escroquerie.

Comment éviter les arnaques sur Internet

Des arnaques, il y a en a plein sur Internet. La toile est infectée par cette gangrène liée à la cupidité et par ces vermines que sont les fameux « black hats » ces chapeaux noirs qui ne cherchent qu'à s'enrichir. Ce qui est surprenant, c'est que nombre de ces arnaques sont utilisées depuis plusieurs années et sont plutôt basiques et faciles à repérer. Ce qui est effrayant, c'est que bon nombre des escrocs d'aujourd'hui agissent comme s'ils représentaient des entreprises établies et légales. Logés dans des pays où il y a peu ou pas de surveillance, opérant dans les zones grises du monde virtuel en utilisant des techniques de sécurité de haut vol qui maintiennent leur anonymat, invisibles et hors de portée des régulateurs et des forces de l'ordre, ces gens ont des bureaux, des secrétaires, proposent des heures d'ouverture, émettent des fiches de paie et prennent même des vacances. Comment éviter les fraudes sur Internet ? C'est généralement facile car nombre d'entre elles sont assez évidentes et, une fois que vous commencez à comprendre les différences entre un vrai site et un faux Web, cela devient une seconde nature.

Les arnaques les plus courantes sur Internet

1. Les options binaire

La fraude numéro un sur Internet est liée aux options binaires. Les options binaires sont une méthode simplifiée de négociation des marchés financiers avec un risque limité et un résultat prédéterminé. Les options binaires elles-mêmes ne sont pas des arnaques. En fait, il s'agit ici de moyens plus faciles de faire des échanges commerciaux qui servent d'instrument spéculatif dans le monde entier. Il existe de nombreuses juridictions, avec notamment la CFTC américaine, la FCA britannique, la CySEC UE/Chypre, la FSA australienne et bien plus encore, qui autorisent, réglementent et supervisent la négociation d'options binaires de type bourse. L'escroquerie vient du fait qu'il y a plus de courtiers non autorisés, de services de signalisation, de personnes qui se disent traders, de pourboires et de gourous que tous les courtiers réglementés que l'on trouve dans le monde, et tout ce qu'ils veulent, c'est vous convaincre de déposer de l'argent pour qu'ils puissent en avoir. Et ils atteignent facilement leurs objectifs car nombreux ceux qui y croient et qui sont ainsi les victimes de pertes qui se montent à plusieurs dizaines de millions de dollars chaque année depuis 2011.

Les options binaires offrent une diversité de fonctionnalités qui attirent les gens qui veulent dépenser de l'argent. Tout d'abord, il y a ceux qui veulent s'enrichir rapidement et qui cherchent toujours une solution facile. Ces gens sont souvent dans une situation difficile pour vouloir gagner ainsi rapidement un peu d'argent ou n'ont tout simplement pas l'éthique nécessaire pour faire le travail qu'il faut pour gagner de l'argent dans des conditions normales. Ils vont faire des recherches sur Internet et trouver des annonces publicitaires qui annoncent des profits rapides, 80% en moins d'une minute, jouer en bourse sur les marchés offrant le plus de liquidités au monde. Ne vous inquiétez pas diront-ils, le commerce des options binaires est facile et si vous avez besoin d'aide – nous avons un gestionnaire de compte, un auto trader, un service de monitoring qui vous aidera à ne pas trop

perdre d'argent juste assez pour vous amuser, vider votre compte et vous inciter à vouloir aller plus loin.

Ensuite viennent les traders frustrés par les autres modes d'actions. Ils ont déjà perdu de l'argent dans le trading d'options standard ou de forex, mais pensent toujours qu'ils peuvent être gagnants. Après tout, il y a toujours quelqu'un qui a gagné tout l'argent qu'il avait perdu, grâce au binaire. C'est facile, le risque/récompense est beaucoup plus simple que le forex au comptant à effet de levier, le courtier vous donnera un bonus d'inscription pour augmenter votre mise (les primes impliquent des exigences qui font qu'il est probable que vous aurez déjà perdu votre liasse de billets avant de les toucher) et vous pouvez aussi utiliser les mêmes techniques que le forex. Et si vous ne pouvez pas l'utiliser, le courtier est sûr d'avoir un signal / autotrader qui peut vous aider. Si vous ne vous êtes pas encore lancé, ne vous inquiétez pas, ils peuvent vous aider à savoir comment vous y prendre.

Le pire concerne l'« autre » catégorie de victimes. Ce sont habituellement des gens qui se sont inscrits pour une chose particulière à un endroit donné, sans savoir que leur nom a été mis sur une liste qui a été vendue sur le Dark Web à des escrocs financiers. Ces personnes peuvent agir à titre individuel ou à partir d'un centre d'appels (voir ma mention sur les escrocs employés de bureaux) et utiliser des « tactiques de marketing à haute pression ». Leurs interlocuteurs sont dociles, sociables et convaincants et ont toujours un contre-argument pour chaque argument, le bon moyen de motiver chaque personne qui pourrait s'opposer à leurs techniques. Leurs cibles sont littéralement les orphelins, les grands-mères, les veuves, les parents célibataires et les étudiants qui peuvent avoir des besoins financiers légitimes qu'un investissement pourrait résoudre. Ils ne sauront probablement pas qu'ils investissent dans des options binaires, ou que leur dépôt est lié par des termes de bonus, ou que le courtier est en fait une arnaque complète qui agit depuis certaines îles tropicales paradisiaques sans respecter une quelconque loi bancaire.

Il est très facile d'éviter ce type d'arnaque. Tout d'abord, si vous savez que ce que vous êtes en train d'étudier des options binaires ou des options binaires liées et que vous n'êtes pas un trader qui recherche un courtier/échange situé dans votre juridiction, vous devriez simplement passer à autre chose et tout oublier. Ce n'est peut-être pas une arnaque, mais c'est probablement le cas. Deuxièmement, si vous subissez des pressions par téléphone, par e-mail ou par tout autre moyen de communication en vue d'un investissement, assurez-vous de bien vérifier les licences, les statuts et les recommandations, et prenez conseil auprès de votre organisme de réglementation local afin de vous assurer que ce que l'on vous propose est bien légal. Ce n'est probablement pas le cas, il y a de nombreuses lois dans presque tous les pays qui empêchent les types d'abus commis par les courtiers et les spécialistes du marketing frauduleux d'options binaires.

2. Sites Clonés

Les sites Web clonés représentent l'arnaque numéro deux sur notre liste des arnaques sur Internet les plus courantes en 2017. Les sites Web clonés sont des sites Web avec une URL, un nom commercial et une apparence qui vous font penser que vous consultez le site d'une entreprise légale mais ce n'est pas le cas. J'ai découvert cela lors de la recherche d'options binaires, mais cela peut s'appliquer à n'importe quelle forme de société financière, d'investissement ou d'entreprise qui accepterait de l'argent du public sur une base régulière. Ils ont installé des ateliers pour faire exactement ce que le nom implique, en copiant une entreprise existante. Au lieu d'accepter votre dépôt pour un placement et de l'appliquer ensuite aux fonds communs de placement, aux sociétés de courtage ou aux actions, l'entreprise prend l'argent et l'investit dans une forme de mauvaise

orientation pour garder les clients occupés jusqu' à pouvoir faire sortir l'argent à leurs dépens. Imaginez que vous allez chercher quelque chose que vous voulez acheter ou dans lequel vous voulez investir sur le net et que vous trouvez un site Web offrant exactement ce que vous voulez. Ajoutez à cela la facilité avec laquelle il est possible de transférer de l'argent sur le Web et le potentiel de fraude devient facilement évident. La meilleure façon d'éviter ces arnaques est d'être vigilant vis-à-vis de tout site Web avec lequel vous voulez effectuer une transaction. Si vous n'êtes pas sûr de son authenticité alors ne l'utilisez pas, je suis sûr que vous pouvez trouver tout ce dont vous avez besoin sur Amazon, mais assurez-vous que le site Web qui ressemble à Amazon appartient effectivement à Amazon.

3. Fausses informations

Les fausses informations sont une grosse arnaque qui fait le tour du monde. Elles sont utilisées pour influencer l'opinion publique et détourner l'attention. Le problème est devenu si marqué que les élèves remettent maintenant en question la véracité de l'information qui leur est enseignée dans les écoles. Ce problème a été mis en lumière pour la première fois, lors des élections américaines de 2016, entraînant une prise de conscience du public. Les retombées de ces fausses informations se font toujours sentir à ce jour, car elles ont semé l'ombre du doute dans les médias et parmi les décideurs gouvernementaux, des deux côtés de l'équation.

4. Email de phishing / Arnaque nigériane

Les arnaques liées à l'hameçonnage par e-mail sont parmi les plus anciennes qui existent sur Internet. Il faut dire que les courriels représentent après tout l'un des tous premiers usages Internet largement utilisé par les entreprises et les particuliers. Alors que beaucoup sont facilement repérables et vont directement dans vos courriers indésirables, certains passent encore à travers les mailles du filet et doivent être filtrés manuellement. L'escroquerie nigériane est la plus commune.

Bonjour, je suis un représentant du prince/gouvernement du Nigeria et j'ai besoin de votre aide. J'essaie de fuir les persécutions et j'ai besoin d'aide pour transférer de l'argent en dehors de mon pays. Si vous m'aidez, je peux vous promettre des sommes d'argent conséquentes. Tout ce que vous devez faire est de m'envoyer quelques milliers de dollars pour démarrer les virements bancaires. Si cela vous intéresse, transférez bla bla bla bla et vous perdez votre argent.

Si vous n'êtes pas en mesure de comprendre que c'est une arnaque en voyant l'expéditeur ou le sujet, jetez un coup d'œil rapide au contenu : les termes marketing ou l'argumentation pour obtenir la miséricorde numérique sont assez faciles à capter. La meilleure façon d'éviter cela est de vous désabonner de la liste à laquelle vous êtes inscrit et de ne plus ouvrir d'e-mails.

5. Arnaques à la carte de vœux

Les escroqueries à la carte de vœux, les escroqueries via un ami et autres escroqueries distribuant des logiciels malveillants par courriel sont anciennes et courantes mais elles restent toujours d'actualité. Autrefois, les logiciels malveillants installaient des fenêtres publicitaires ou des barres d'outils gênantes et difficiles à supprimer. De nos jours, ces petits virus nuisibles sont capables de faire beaucoup plus de dégâts et pourraient même infiltrer votre réseau domestique ou professionnel et le compromettre. Comme pour les arnaques liées à l'hameçonnage, la meilleure façon de les éviter est de ne pas ouvrir ce type de mail, à moins d'être absolument sûr de savoir qui l'a envoyé et d'où ils proviennent. Si vous pensez que vous devez l'ouvrir, utilisez un ordinateur virtuel ou une machine virtuelle pour le faire. Une machine virtuelle est un système d'exploitation installé sur un autre système d'exploitation, généralement accessible via le Web, et est un environnement

stérile/sécuritaire dans lequel les menaces potentielles de logiciels malveillants peuvent être ouvertes. L'utilisation d'un programme anti logiciels malveillants et d'un antivirus est également très importante.

6. Arnaques à la loterie

Les arnaques à la loterie sont un autre de ces stratagèmes anciens qu'utilisent les cybercriminels et qui sont perpétrées sur Internet via courriel. L'arnaque à la loterie fonctionne en jouant sur l'avidité et les rêves de richesse instantanée. Qui n'a pas rêvé de gagner à la loterie et ces gens qui vous font miroiter cela vous facilitent la tâche en vous disant de ne pas vous inquiéter si vous ne vous souvenez pas avoir acheté un billet de loterie lorsque vous avez fait bla-bla sur Facebook/Instagram/Pinterest ou un autre site de réseaux sociaux. Tout ce que vous devez faire pour réclamer votre prix, c'est de vérifier vos données financières et leur envoyer une petite somme. Ils peuvent ensuite vider vos comptes de tout ce que vous avez et disparaître de la surface de la terre. C'est assez facile d'éviter cette arnaque, si vous ne possédez pas un billet de loterie dans votre main ou si vous ne vous souvenez pas avoir participé à un concours, vous n'avez certainement pas gagné.

7. Fausses arnaques à l'antivirus

C'est une autre vieille astuce qui fonctionne bien. Vous surfez sur le net et soudain, une fenêtre sous forme de pop-up apparaît vous indiquant que votre ordinateur est infecté. La bonne nouvelle, c'est que vous pouvez télécharger cet antivirus dès maintenant pour le nettoyer sans difficulté. Ce qu'ils ne vous disent pas, c'est que la fenêtre pop-up que vous venez de voir est en fait un virus que vous allez lancer. Les logiciels téléchargés peuvent supprimer les menaces « malveillantes », mais ils peuvent également exploiter votre ordinateur et vos périphériques pour récupérer toutes les données qu'ils peuvent trouver, puis les renvoyer à une base centrale. Ce qui les rend très efficaces vis-à-vis de leurs proies, c'est le fait qu'ils arrivent à se faire passer pour un message de Norton, McAffee ou tout autre service de confiance. Le pire correspond au rançongiciel si redouté qui verrouillera votre ordinateur à moins que vous n'achetiez leur « service ».

Comment repérer une arnaque en ligne

Les arnaques prennent de nombreuses formes et les arnaqueurs d'aujourd'hui sont plutôt rusés. Certaines arnaques sont très complexes et peuvent même inclure des sites Web complémentaires mis en place pour confirmer et valider l'arnaque de départ. C'est chose courante dans le cas de fraude financière, lorsqu'un faux organisme de réglementation ou de surveillance est établi pour vérifier la légitimité d'un courtier ou d'un gestionnaire.

Collectez des informations.

Une entreprise légale vous fournira une quantité abondante de renseignements sur elle-même. Vous voudrez voir les adresses, les numéros de téléphone, les e-mails et bien plus encore. Une fois que vous aurez trouvé ces infos, vous devrez en vérifier la véracité. Il y a des centaines de bureaux virtuels dans le monde entier, les entreprises peuvent ainsi ouvrir un compte pour le courrier postal et s'en servir comme siège social de sociétés et d'autres entités commerciales légales. Les cybercriminels aiment les utiliser pour de nombreuses raisons, y compris la réglementation/légalité implicite en lien avec le pays d'origine.

Ce qu'ils offrent est-il trop beau pour être vrai ?

Comme on le dit, si c'est trop beau pour être vrai, c'est probablement le cas. Les escrocs et les sites frauduleux aiment offrir des choses qu'ils ne peuvent pas garantir comme les profits, les taux de profit, une garantie de remboursement si vous perdez / si cela ne fonctionne pas et tout ce qu'il faut pour gagner votre confiance. Les entreprises légales n'offrent généralement pas ce genre de choses, surtout les entreprises financières.

Annoncent-ils fonctionner sous couvert de la réglementation, être officiellement déclarés ou recommandés ?

N'oubliez pas de vérifier aussi cela et faîtes plus qu'une visite rapide des sites Web. Trop souvent, surtout si l'arnaque réussit financièrement pour le fraudeur, des sites Web peuvent même être établis pour aider à faire croire à la véracité de ces éléments. Un organisme de réglementation peut dire que le service est juridiquement opérationnel et digne de confiance, un auditeur peut dire que le site est de qualité et qu'il répond à tout ce qu'il annonce, mais s'il n'est pas réel, cela ne vaut pas le temps qu'il a fallu pour le consulter.

Demandent-ils de l'argent ?

Sauf si vous échangez avec une association caritative, il n'existe aucune raison pour laquelle une entreprise, un jeu-concours ou une offre d'emploi légitime vous obligerait à donner d'abord de l'argent. Si l'on vous demande ou si l'on vous presse d'envoyer ou de déposer de l'argent, c'est une alerte qui ne doit pas être négligée. Si vous n'avez pas déjà vérifié avec qui vous êtes en contact, vous devriez le faire.

Comment éviter les arnaques les plus courantes sur Internet

La meilleure façon d'éviter les arnaques, les fraudes, les cyberpirates et les attaques de logiciels malveillants qui circulent sur Internet est d'utiliser les techniques de chapeau noir à leur encontre. L'un des principaux outils qu'ils utilisent eux-mêmes aujourd'hui vient des grandes entreprises et du gouvernement, afin de sécuriser les connexions Internet et protéger les données : cela s'appelle un Virtual Private Network. Un VPN ou réseau privé virtuel est un moyen d'assurer l'intégrité des connexions Internet et la sécurité des données transmises. Dans le passé, ils n'étaient utilisés que par ces mêmes grandes entreprises en raison de leur complexité d'installation. Découvrez en davantage sur les bénéfices liés à l'utilisation d'un VPN en termes de sécurité.

Maintenant disponibles pour le grand public, les VPN sont rapidement devenus la norme en matière de sécurité pour la maison et le bureau. Leur fonctionnement est simple. Vous, l'utilisateur, téléchargez le logiciel VPN sur votre appareil qu'il s'agisse d'un Mac, PC, Android, iOS ou autre. Le fournisseur de services VPN installe et gère un réseau de serveurs VPN dédiés. Lorsque vous utilisez le VPN pour vous connecter au serveur, cela crée un tunnel digital via lequel votre connexion s'établit, le tunnel est virtuellement impossible à détecter et s'il est détecté, impossible à pirater car il est crypté.

L'objectif cible d'un VPN est la sécurité de la connexion, les bénéfices secondaires involontaires comprennent l'anonymat sur Internet. La combinaison de ces deux éléments rend impossible la détection de logiciels malveillants, à moins que vous ne tombiez sur eux volontairement ou involontairement. Il rend également impossible pour les chapeaux noirs et les pirates malveillants de tracer votre connexion, ou d' y accéder pour accéder à vos informations. La seule chose contre laquelle un VPN ne peut pas vous protéger, c'est vous-même. Apprenez-en davantage sur les erreurs courantes en matière de sécurité Internet et comment les éviter.

Si vous utilisez Internet, vous avez besoin du VPN et Le VPN est le meilleur choix qui existe aujourd'hui. L'entreprise possède un réseau de serveurs VPN dans plus de 114 pays dans le monde et propose des tarifs à partir de 4,95€ par mois, alors pourquoi attendre, abonnez-vous à Le VPN avant qu'il ne soit trop tard.

Exemples d'arnaques par Courriel

Arnaque au remboursement d'amende / faux site GPE

Un spam promet aux internautes un remboursement d' amende en imitant le site du GPE

Un remboursement d'amende ? Quelle aubaine, vous vous étiez justement fait prendre par un radar récemment ! Malheureusement, il s'agit d'une nouvelle tentative d'arnaque.

Tout commence par la réception d'un mail provenant de ne-pas-repondre@amendes.fr et indiquant que, suite à une erreur technique sur un radar, il est possible d'être remboursé d'une amende payée suite à une infraction au code de la route.

On pourrait déjà remarquer les fautes d'orthographe du courriel ainsi reçu. Mais beaucoup remarqueront le lien présent dans le courriel. Il renvoie vers un site qui est en fait une copie quasi conforme du site officiel https://www.creances-publiques.fr/

Arnaque avec le nom de SFR


SFR

Certifié SFR

LE SERVICE CLIENT,
TOUJOURS À VOS CÔTÉS

Bonjour,

Des difficultés d'authentification sont survenues dans votre messagerie.
Veuillez respecter la procédure en (Cliquant ici Messagerie/sfr.fr) » pour vous identifier au plus vite. (identification obligatoire)

Afin d'éviter que votre messagerie soit bloqué.

Nous sommes là pour vous et à tout moment sur sfr.fr rubrique Espace Client

À très bientôt
L'équipe SFR Mail

Si nous mettons notre curseur sur le lien **sans cliquer** nous voyons l'adresse du lien

(Cliquant ici Messagerie/sfr.fr)

https://s.yam.com/3eBxx

Arnaque avec le nom aléatoire

Bonjour jean@laposte.net

Nous avons bien reçu votre commande N°50128348 du 18/05/2018 et vous adressons ci-joint un duplicata de votre facture.
Vous pouvez télécharger votre duplicata à cette adresse :
Télécharger le duplicata

Des questions ? Nous sommes joignables du Lundi au Vendredi de 7h à 19h au numéro indiqué sur l'en-tête votre facture.

En vous remerciant de votre fidélité.

Cordialement,
Comptabilité SARL ETIENNE

Bonjour association@laposte.net

Nous avons bien reçu votre commande N°50128348 du 18/05/2018 et vous adressons ci-joint un duplicata de votre facture.
Vous pouvez télécharger votre duplicata à cette adresse :
Télécharger le duplicata

Des questions ? Nous sommes joignables du Lundi au Vendredi de 7h à 19h au numéro indiqué sur l'en-tête votre facture.

En vous remerciant de votre fidélité.

Cordialement,
Comptabilité SARL LEGRAND

Bonjour association@laposte.net,

Nous vous faisons parvenir ci-joint la facture liée à votre commande du Lundi 15 Avril 2018.

Votre facture est disponible à l'adresse suivante: Télécharger ma facture

Nous vous remercions de la confiance que vous nous accordez.

___

Désabonnez-vous

Arnaque avec le nom Française des jeux

Bonjour,

Chère cliente, cher client,

Nous vous informons que vous venɛz dɛ remporter une somme très importante.

Pour plus d'information consultɛr les pièces jointes.

Pour la marchɛ à suivrɛ contactɛr Maître DAVID JAMES par émaiL

Vous trouvɛrɛz son adrɛsse dans les fichiɛrs.

Bonne réception

FRANÇAISE DES JEUX
N° de LOT: 9001-BNK-87
N°de Réf: 07/04/1990

Arnaque avec le nom des impots

Réagissez ! SIGNALER.

https://www.internet-signalement.gouv.fr/

Internet est un espace de liberté où chacun peut communiquer et s'épanouir. Les droits de tous doivent y être respectés, pour que la « toile » reste un espace d'échanges et de respect. C'est pourquoi les pouvoirs publics mettent ce portail à votre disposition. En cliquant sur le bouton « SIGNALER », vous pouvez transmettre des signalements de contenus ou de comportements illicites auxquels vous vous seriez retrouvés confrontés au cours de votre utilisation d'Internet.