Face à la recrudescence des arnaques en tous genres, le CIM.PP à décidé d'y consacrer un dossier permanent pour vous tenir informé sur les nouvelles inventions des ' pirates ou escrocs '*(via internet ou non)* ! et croyez-le, ils ne manquent pas d'imagination !

Vous avez reçu un mail gagnant de la loterie alors que vous n'avez participé à aucun jeu, un SMS douteux de l'Assurance maladie concernant le renouvellement de votre carte vitale ou encore un coup de fil d'un conseiller bancaire dont vous ne reconnaissez pas la voix ?

Il est fort probable que vous soyez la cible d'une tentative d'arnaque. Les escroqueries sont extrêmement fréquentes en ce moment et prennent différentes formes, les aigrefins ne manquant pas d'imagination pour piéger leurs victimes.

De plus, la numérisation de la société représente une aubaine pour les escrocs, qui peuvent cibler des personnes sur les réseaux sociaux et récupérer leurs données personnelles (adresses, coordonnées bancaires) sur le darknet entre autres.

Agissant depuis l'étranger pour la plupart, les arnaqueurs sont difficiles à coincer malgré les nombreux signalements.

Que vous ayez déjà été victime d'une escroquerie ou que vous soyez passés entre les mailles du filet, ce document vous permettra de connaître les arnaques qui circulent le plus en ce moment, afin de mieux les anticiper.

Quelques explications sont données sur ces arnaques dont certaines sont bien connues

En règle générale, ne cliquez jamais sur un lien (téléphone, tablette ou ordinateur), même par simple curiosité, sans avoir pu vérifier la validité de la chose.

Les arnaques les plus courantes dont vous devez vous méfier (les « tops » en gras rouge)

2022/2023

- ***à la carte vitale***
- ***à l'indemnité inflation***
- Faux conseiller bancaire
- ***à la rénovation énergétique***
- au mail de la police luxembourgeois
- à la carte prépayée
- De faux policiers arnaquent à l'aide de coupons PCS
- ***au remboursement d'impôts***
- ***à la Française des jeux (FDJ)***
- aux faux mail de Lidl
- aux NFT (cryptomonnaie)
- au Service civique
- aux fausses infirmières
- aux placements financiers
- ***au Compte personnel de formation (CPF)***
- Uber Eats : l'arnaque aux faux restaurants
- à la vente et à la location immobilière
- ***aux dons pour l'Ukraine***
- des jeunes au pair
- à l'irlandaise
- au matelas
- à la fiente d'oiseau
- à la greffe
- Consommation d'énergie
- ***Vignette Crit'air***
- Urgence familiale
- ***A la carte SIM***
- ***….***

Arnaque à la carte vitale

Par SMS ou par mail, des escrocs tentent d'arnaquer des particuliers en leur proposant de renouveler leur carte vitale tout en usurpant le logo de l'Assurance maladie pour gagner leur confiance. Le hic, c'est que l'assurance maladie assure qu'il "n'existe pas de campagne pour obtenir une nouvelle carte vitale".

L'escroc vous incite à remplir un formulaire afin de continuer à être couvert via ameli-vital.fr. Cela lui permet de récupérer des informations personnelles à votre sujet, comme des données bancaires par exemple, chose que l'Assurance maladie ne vous demandera jamais pour vous envoyer votre nouvelle carte vitale

. Cette dernière envoie régulièrement des messages de prévention afin que les cibles de ces faux SMS et mails soient particulièrement prudentes.

Arnaque à l'indemnité inflation

La caisse nationale d'allocation familiale (Cnaf) a également été touchée par le phénomène d'hameçonnage, également prénommé "phishing".

Le 4 février 2022, la Cnaf alertait que des mails frauduleux circulaient dans les boîtes mail de plusieurs personnes, promettant une indemnité inflation versée à hauteur de 387 euros alors que cette prime s'élève en réalité à 100 euros.

Comme pour l'arnaque à la carte vitale, un lien est présent dans le mail, affichant une page sur laquelle il est demandé de remplir un formulaire afin de toucher la somme.

Faux conseiller bancaire

Au début du mois de février 2022, la Banque de France alertait sur l'augmentation des fraudes émanant de faux conseillers bancaires.

Les escrocs utilisent des "techniques de manipulation qui visent à amener leurs victimes à valider elles-mêmes les opérations frauduleuses". Les cyberdélinquants commencent par se renseigner sur la potentielle victime via du "phishing" ("hameçonnage" en français), des "malwares" (ces "logiciels hostiles") ou en achetant des fichiers remplis des données personnelles de la proie, sur le dark web.

Arnaque au mail de la police ‘ luxembourgeoise ‘

Le 26 janvier dernier, la police luxembourgeoise alertait sur la circulation d’une arnaque au faux mail dans le pays. Les aigrefins envoyaient des courriels frauduleux, prétendument signés par le directeur général de la police, qui concernent une procédure d’enquête pénale.

Le texte demande aux victimes d'envoyer leurs justifications sur une adresse Gmail, en menaçant de poursuites. Mais la police locale assure qu’elle ne procède pas de la sorte pour convoquer des particuliers et qu’il s’agit d’une vaste escroquerie. De plus, des éléments dans le document permettent rapidement de se douter qu’il s’agit d’une arnaque, comme de grossières fautes de frappe par exemple. Les forces de l’ordre vous invitent donc à mettre ce mail directement dans la corbeille si vous le recevez.

Le même ,phénomène s’est produit en France

Arnaque à la rénovation énergétique

Le développement des aides à la rénovation énergétique comme MaPrimeRénov' a donné un véritable coups de pouce aux Français, qui ont multiplié leurs travaux d'énergie. Mais voilà, quand un phénomène prend de l'ampleur, **les arnaqueurs ne sont jamais bien loin pour s'en emparer.**

Dans la rénovation énergétique, **les escroqueries vont bon train et l'aide MaPrimeRénov' à particulièrement** été utilisée comme outil par les escrocs. En général, ils avancent l'argument de la complexité des démarches à faire à leurs victimes, pour les effectuer à leur place et instaurer leur piège.

Dans le même cas de figure, les arnaques à l'isolation ne sont pas en reste.

L'un des grands classiques est l'arnaque à 1 euro. La situation dégénère généralement lorsque l'entreprise frauduleuse demande d'avancer des frais, en promettant un remboursement par la suite. Certaines personnes finissent ainsi par souscrire des prêts à la consommation de plusieurs milliers d'euros. Autre risque, des travaux mal effectués, qui obligent les ménages à payer des frais supplémentaires pour réparer ces malfaçons.

Ces escroqueries sont courantes dans la rénovation énergétique, ne laissez donc jamais un professionnel se charger d'entamer les démarches à votre place, sans aucune facture ou trace des documents. Méfiez-vous aussi des entreprises prétendant être mandatées par un organisme public, car les services publics ne démarchent jamais, que ce soit par internet, par téléphone ou au domicile. Fuyez les entreprises qui démarchent de manière abusive et agressive au téléphone et qui vous menacent de pénalités. Effectuez des recherches sur la société qui se présente au bout du fil, lisez bien toutes les dispositions qui figurent sur le contrat, et enfin ne signez jamais dans la précipitation.

De faux policiers arnaquent à l'aide de coupons PCS

Usurper l'identité des forces de l'ordre semble être une stratégie privilégiée par les escrocs. Récemment, ce sont les habitants de Clermont-Ferrand et Reims qui en ont fait les frais.

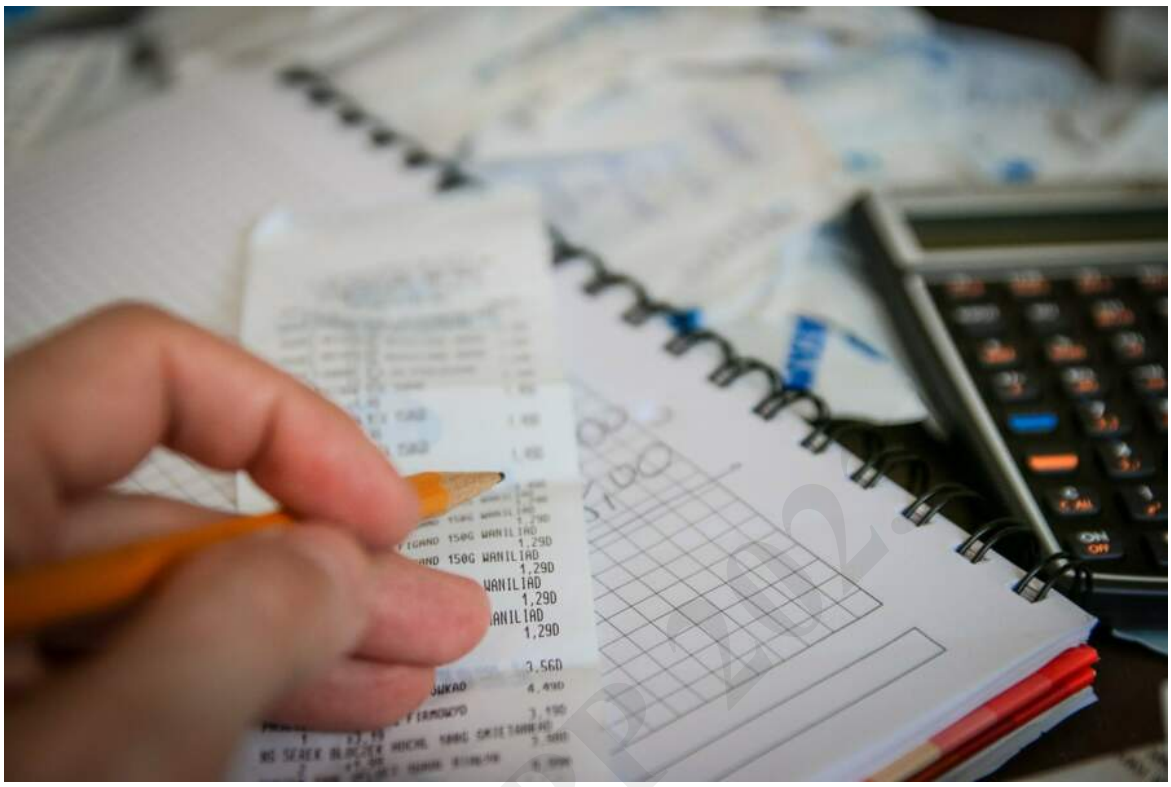
Concernant la capitale du département du Puy-de-Dôme, un article de France Bleu publié le 2 mars a révélé que cinq plaintes ont été déposées au commissariat central de la ville le 1er mars. De faux policiers auraient soutiré plus de 5.000 euros à leurs victimes en utilisant l'arnaque aux coupons PCS. Ces coupons, qui peuvent aller de 20 à 250 euros, peuvent être achetés dans des bureaux de tabac. Ils fonctionnent comme des cartes de paiement prépayées, permettant de réaliser des achats sécurisés sans donner ses coordonnées bancaires.

Ce procédé bien connu des services de police consiste à téléphoner à des personnes vulnérables, souvent âgées, en se faisant passer pour des policiers enquêtant sur des personnes des pays de l'Est.

L'arnaque à la carte prépayée

Ici, la méthode se rapproche de l'arnaque aux coupons PCS mise en place par les faux policiers. Comme pour les coupons, la carte prépayée permet à ses utilisateurs de réaliser une transaction sans avoir besoin d'entrer des informations bancaires.

C'est une des alternatives les plus simples pour payer en ligne. Problème : les escrocs se servent de cette simplicité pour agir et deux tiers des fraudes qui ont lieu sur Internet sont des arnaques à la carte prépayée,



Arnaque au remboursement d’impôts

À la fin de l’année 2021, des courriers électroniques circulaient dans les boîtes mail des contribuables avec pour objet des remboursements d’impôts.

Il s’agit en réalité de tentative d'arnaque, prenant la forme de phishing (hameçonnage). Selon l’UFC-Que choisir qui alertait sur cette escroquerie le 22 novembre 2021, le message arbore l’entête du site officiel des impôts : impots.gouv.fr, gage de crédibilité, mais la démarche ne provient en aucun cas du fisc. Dans le texte, il est indiqué qu’il suffit de cliquer sur le lien fourni et de remplir un "formulaire de remboursement" afin de récupérer la somme.

Il est ensuite demandé de renseigner plusieurs informations relatives à votre identité, puis le site vous amène sur une autre page en vous invitant à entrer les coordonnées d'une carte bancaire.

Les arnaques à la Française des jeux

C'est l'une des arnaques les plus courantes du circuit de l'escroquerie. L'arnaque aux jeux de la FDJ consiste à envoyer un mail à un particulier en lui faisant croire qu'il a été tiré au sort et qu'il a remporté une coquette somme d'argent. Dans un document joint avec le courriel, l'aigrefin se fait passer pour la FDJ en reprenant ses couleurs et en mentionnant le logo de l'Euromillion, du Loto de My Million et d'autres jeux célèbres afin de paraître crédible.

Pour récupérer le gain, l'arnaqueur invite la cible à répondre le plus rapidement possible au mail envoyé en communiquant ses informations personnelles. Ensuite, pour gagner sa confiance, il est mentionné que ses données seront transmises à un avocat ou un huissier de justice, qui se chargera d'indiquer la procédure à suivre pour récupérer l'argent. Dénommé phishing, ce type d'arnaque peut également être transmis par SMS ou MMS, même si les mails restent le canal privilégié par les escrocs.

Pour ne pas se faire duper, il existe plusieurs failles que vous pouvez facilement repérer dans le document. Les fautes d'orthographe, le caractère flou des images et des logos ainsi que la photo au format écrasé ainsi que la signature de Stéphane Pallez (PDG de la FDJ) en fin de document sèment le doute, **car elle ne signe jamais de courrier pour féliciter un gagnant**.

Enfin et surtout, la FDJ rappelle sur son site qu'il est impossible de gagner un lot ou un gain à une loterie "si l'on n'a pas acheté un ticket ou joué en ligne".

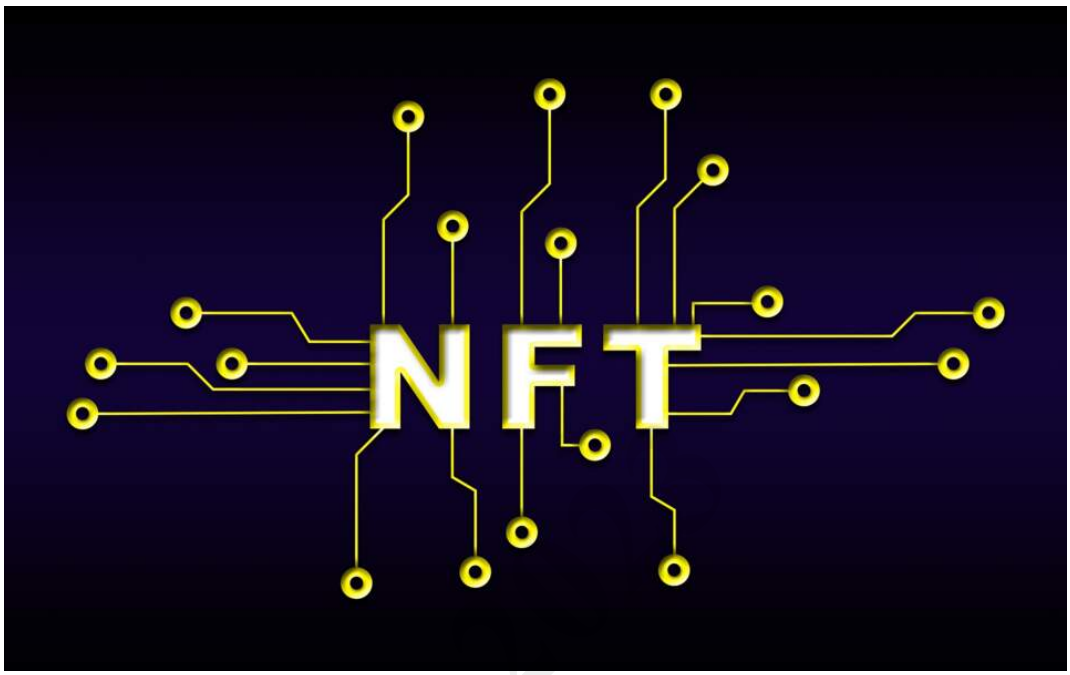
L’arnaque au faux mail de Lidl

Le 15 novembre 2021, le média spécialisé Numerama alertait sur une tentative d’arnaque à travers un faux mail d’hameçonnage, supposément envoyé par Lidl.

Dans le courriel, il est expliqué au destinataire qu’il a été sélectionné dans le but d'”obtenir une offre exclusive”, vous permettant de gagner des lots comme un iPhone 12 par exemple. Pour en bénéficier, il suffit alors de remplir un bref questionnaire sur le site de Lidl, au moyen d'un lien fourni dans l'email.

Mais voilà, l’URL n’est en rien associée à l’enseigne allemande de grande distribution. Il s’agit d’une tentative de phishing dont le but est de récupérer des informations personnelles, telles que nom, numéro de téléphone, adresse postale…

mais également des informations bancaires que vous aurez transmises à travers des formulaires. Si vous recevez un mail de Lidl vous assurant que vous êtes sélectionné pour remporter des cadeaux alléchants, méfiez-vous donc un escroc se cache certainement derrière l’offre.



L'arnaque aux NFT (jeton cryptographique)

Les NFT (jeton non fongible, NDLR) ont tellement la cote que même les escrocs se sont emparés du phénomène pour mettre en place des stratagèmes d'arnaque. Des utilisateurs de Fractal, une plateforme en ligne permettant d'acheter et de revendre des NFT, en ont fait l'amère expérience en fin d'année 2021. Selon Le Figaro et Phonandroid, le 21 décembre dernier, des hackers ont réussi à pirater le compte Discord de certains salariés de Fractal.

Grâce aux accès de ces salariés, les pirates ont pu poster une annonce frauduleuse. "Nous allons mettre en vente 3.333 NFT qui vont rapidement partir (…). N'oubliez pas, vous ne pouvez payer qu'avec la cryptomonnaie Solana", précisait l'annonce. Sur 100.000 utilisateurs de la plateforme, 300 sont tombés dans le panneau et les aigrefins sont parvenus à siphonner 800 jetons de cryptomonnaie Solana, l'équivalent de 130.000 euros. Encore totalement inconnus pour certains, les systèmes de cryptomonnaies et NFT peuvent être difficiles à appréhender et les arnaqueurs spécialistes en profitent pour sévir.

S'ils sont réputés pour leur sécurité, certains blockchains peuvent avoir des failles, vérifiez donc toujours la fiabilité d'une offre NFT avant d'en acquérir.

L’arnaque au Service civique

Ouvert à tous les jeunes de 16 à 25 ans (jusqu’à 30 ans pour les jeunes en situation de handicap), le service civique est un engagement volontaire dans une mission d’une durée de 6 à 12 mois, au service de l'intérêt général et sans condition de diplôme.

Cette mission est indemnisée entre 580,72 euros et 688,40 euros net par mois. Une indemnité de 473,04 euros net par mois (522,87 euros brut) est versée au volontaire par l’État, alors que l’association qui le prend en charge verse le complément de revenus. Cependant, victimes d’une escroquerie, certains jeunes ont vu leur salaire leur passer sous le nez.

L’arnaque *a*ux fausses infirmières

Se cacher derrière une profession digne de de confiance comme celle d’infirmière est une stratégie privilégiée par les escrocs. Ici, et comme dans la majorité des arnaques, ce sont les personnes âgées et vulnérables qui sont majoritairement visées.

Si vous vous retrouvez face à une infirmière au comportement douteux, il est conseillé d'exiger de cette personne la présentation d'une carte professionnelle de santé. De plus, ne donnez pas d'argent ou vos coordonnées bancaires à quiconque les demanderaient qui ne seraient pas en mesure de s'identifier professionnellement de façon officielle.

Les arnaques aux placements financiers

Les arnaqueurs ciblent bien des domaines pour s'attaquer aux épargnants, mais certains rapportent plus que d'autres. Sur la période 2020-2021, les plus lourdes pertes étaient observables sur des arnaques aux crédits, cryptosactifs, Forex (investissement sur le marché des changes), des fausses offres d'investissement dans des places de parking d'aéroport ou dans des chambres d'EHPAD et enfin des arnaques au livret d'épargne.

Pour chaque domaine, le mode opératoire des arnaqueurs aux placements financiers est relativement identique. Généralement, les épargnants sont interpellés par des publicités mensongères sur Internet, à travers les réseaux sociaux, les boîtes mail, mais aussi sur les applications mobiles de messagerie.

L’arnaque à la vente de véhicules sur Leboncoin

Depuis novembre 2021, un escroc fait rage sur Leboncoin en Haute-Garonne, à en croire les propos de La Dépêche. Il aurait déjà piégé une cinquantaine de victimes et il se pourrait qu’il élargisse son escroquerie sur tout le territoire. D'après les témoignages recueillis par nos confrères de la presse régionale, le mode opératoire est toujours le même. Des Français font leurs recherches sur des sites de particuliers, tombent sur une annonce qui les intéresse, et se décident à contacter le vendeur.

Celui-ci se présente comme un "professionnel", avec un numéro de siret. L’une des victimes raconte comment elle s’est fait berner. L'escroc lui explique qu'il est courtier en automobile, raison pour laquelle les tarifs affichés sont un peu moins chers. Le véhicule est à l'étranger, mais il devrait arriver sous peu. Pour cela, il faut verser un acompte (en général 10% du prix total). Reste donc le dernier paiement à effectuer, le solde, seule manière de faire arriver la voiture en France. L'homme paye, et il est trop tard. Malgré quelques fausses justifications de l'escroc, il ne reprendra plus jamais contact. L'acheteur a perdu 27.780 euros.

L’arnaque au Compte personnel de formation (CPF)

Le Compte personnel de Formation (CPF) permet à toute personne active, dès son entrée sur le marché du travail et jusqu’à la date à laquelle elle fait valoir l’ensemble de ses droits à la retraite, d’acquérir des droits à la formation tout au long de sa vie professionnelle. Cela peut être de la formation à la photographie, au design ou community management entre autres.

Depuis plusieurs mois, de nombreux Français sont harcelés par téléphone par des escrocs qui leur indiquent que leurs droits au CPF sont sur le point d’expirer, et les invitent à payer au plus vite une formation factice ou piratent directement leur compte. **C’est devenu l’arnaque du moment et en un an, elle a augmenté de 200%, selon le rapport annuel de Cybermalveillance.gouv.fr.**

Uber Eats : l’arnaque aux faux restaurants

Des arnaqueurs semblent œuvrer sur les plateformes de livraison en créant des profils de faux restaurants. Un journaliste d’Actu Yvelines a affirmé le 4 mars dernier en avoir été victime. Pour sa commande, le journaliste a choisi l’enseigne "Big Burger’s", qu’il ne connaît pas, mais il est très vite attiré par des "photos de burgers copieux", "une offre promotionnelle sur le dessert" et le "faible montant des frais de livraison. S’il imaginé passer une bonne soirée en dégustant un délicieux burger, sa commande n’arrivera jamais.

Avant de commander à manger sur une plateforme de livraison, assurez-vous bien de l’existence du restaurant auprès duquel vous passez commande en vérifiant son adresse sur internet et les avis Google ou Tripadvisor. Si vous ne trouvez aucune trace de l’établissement, vous avez probablement affaire à une arnaque

Arnaque à la vente et à la location immobilière

Les marchés de la location et de la vente immobilière ne sont pas épargnés par les tentatives d'arnaque. Les victimes peuvent être des vacanciers à travers des locations saisonnières ou des particuliers qui souhaitent louer ou acheter un bien pour y vivre.

Sur ce point, de plus en plus de locataires ou acquéreurs en quête de la perle rare décident de ne pas passer par une agence immobilière pour limiter leurs frais, mais ils se retrouvent davantage exposés au risque d'escroquerie.

Pour amorcer leurs pièges, les arnaques mettent en ligne une annonce pour un appartement ou une maison, sur un site comme Leboncoin, où les vérifications sont faibles. La plupart du temps, ils récupèrent des photos et un texte d'un appartement ou d'une maison qui était auparavant en location ou à la vente.

Les arnaques aux dons pour l'Ukraine

Depuis le début du conflit Russo-ukrainien qui émeut la terre entière, les élans de solidarités se multiplient. Mais malheureusement, parmi les réels appels aux dons, se cachent des aigrefins qui utilisent la guerre pour s'enrichir sur le dos de personnes généreuses. Bogdan Botezatu a tiré la sonnette d'alarme auprès de nos confrères du Figaro. Celui qui est directeur de recherche chez Bitdefender, une société de cybersécurité qui a publié une étude sur le phénomène, explique que les arnaqueurs peuvent adopter plusieurs techniques d'approche : Tout d'abord le traditionnel et indémodable méthode du phishing, qui consiste à duper un internaute pour l'inciter à communiquer ses données bancaires.

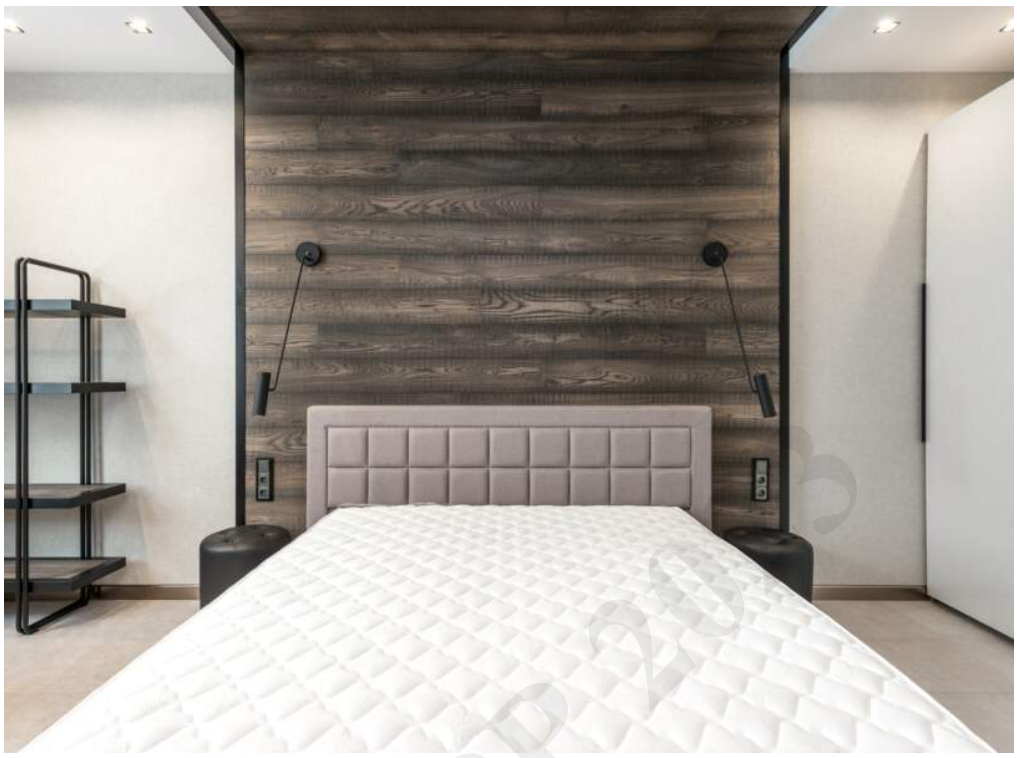
L'arnaque se présente souvent sous la forme d'un message soi-disant envoyé par un citoyen ukrainien réclamant une aide financière pour quitter le pays. Plusieurs milliers d'e-mails frauduleux de ce type ont été envoyés en Europe, en Asie et aux États-Unis. Certains escrocs ont également réussi à usurper les comptes d'utilisateurs ukrainiens sur les réseaux sociaux. À partir de ceux-ci, ils ont envoyé des messages à leurs proches leur réclamant de l'argent pour acheter de la nourriture ou tout simplement pour s'échapper du pays. Par ailleurs, Bitdefender a également repéré la création de faux sites se faisant passer pour des organisations d'aide humanitaire et qui proposent des collectes de fonds. Souvent, le paiement se fait par cryptomonnaie, car l'anonymat du malfrat est préservé, ou par PayPal. Sauf que, comme le souligne Le Figaro, les citoyens ukrainiens ne peuvent pas recevoir d'argent du service PayPal.

L’arnaque des jeunes au pair

Alors avant de vous lancer dans une aventure de jeune au pair, vérifiez bien la fiabilité de votre famille. N’avancez surtout pas d’argent pour financer votre visa et vos billets d’avion, regardez les recommandations liées à votre potentielle future famille d’accueil sur les plateformes de recherche, contactez d’anciens jeunes au pair qui ont fréquenté le foyer en question pour avoir des retours sur expérience et assurez-vous d’avoir un entretien téléphonique, voire même vidéo, avec la famille pour vous assurez de son existence.

L'arnaque à l'irlandaise

Les escrocs se font passer pour des touristes britanniques et s'en prennent à des automobilistes sur des aires d'autoroute. Ils expliquent être de retour de vacances et avoir été dépouillés. Parlant anglais couramment, ils précisent qu'ils doivent rentrer chez eux, mais qu'ils n'ont plus rien et qu'ils doivent être aidés financièrement. La suite de l'arnaque est simple : après avoir pris soin de donner des renseignements personnels qui sont bien évidemment faux, ils demandent un virement instantané à la victime, qu'ils promettent de rembourser une fois la Manche traversée. Ils disparaissent ensuite dans la nature, sans jamais renvoyer l'argent.



L'arnaque au matelas

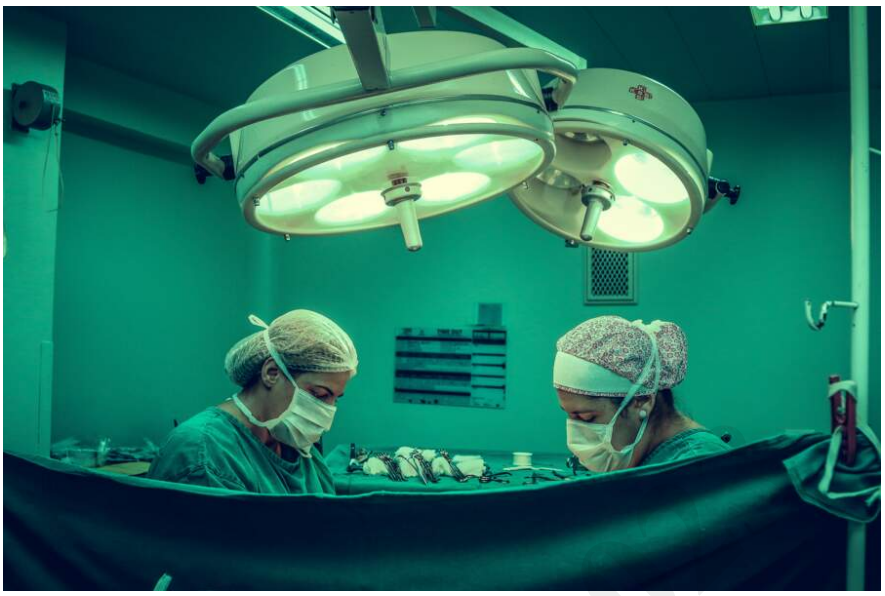
Une fois de plus, les personnes âgées sont visées dans ce type d'arnaque bien connu des commerçants malveillants. Les escrocs font croire à leurs victimes que leur matelas haut de gamme doit être changé. Par chance, ils en ont en stock dans leur camion ! Sauf que ce sont des matelas de mauvaise qualité, qu'ils échangent en demandant parfois une somme d'argent exorbitante.

Les aigrefins usurpent généralement l'identité d'une enseigne de literie reconnue, comme cela à été le cas dans le Calvados, en février dernier. C'est la marque Meubles Dupuis, située à Falaise (14 000) qui en a fait la fâcheuse expérience. Les escrocs se sont fait passer pour le responsable du magasin ou ses collègues : "Ils indiquent qu'un fournisseur les a appelés pour les informer qu'il y avait un problème avec leur matelas, qu'un lot a été déclaré défectueux et qu'ils doivent vérifier si leur matelas est à changer", expliquait le patron à nos confrères de. D'autres escrocs enfilent également une casquette de vendeur indépendant, proposent des matelas à une centaine d'euros sur le marché, mais une fois arrivés chez les clients pour les livrer, ils présentent une facture dix fois plus élevée, prétextant que 100 euros n'est pas le prix du matelas, mais bien le prix de la remise pour reprendre l'ancien.

Pour éviter de vous faire avoir, privilégiez l'achat de votre nouveau matelas directement dans les circuits de vente traditionnels, ignorez les démarchages et ne laissez personne s'introduire chez vous.

L’arnaque à la fiente d’oiseau

Non, il ne s’agit pas là d’une plaisanterie. Certains escrocs utilisent bien une imitation d’excréments de volatiles pour duper leur victime. C’est dans l’Hérault que la gendarmerie a récemment fait état de ce nouveau type d’arnaque pour le moins cocasse. Le mode opératoire est enfantin et laisse sans voix : les malfaiteurs aspergent leur victime d'un liquide qui ressemble à une fiente d'oiseau. La personne tente alors de se retourner et cherche la tâche. Pendant ce temps-là, les individus agissent rapidement, volent le sac à main, le portefeuille ou la carte bancaire de leur cible.



L'arnaque à la greffe

Certains sont prêts à tout pour soutirer de l'argent, même à monter de fausses associations caritatives afin d'obtenir une greffe.

C'est l'idée qu'a eu un couple de Haute-Savoie, résidant en banlieue d'Annecy. Les amoureux ont joué la carte de l'émotion afin de récolter de l'argent facilement, et ont utilisé leur fille âgée de 18 mois comme appât ! "L'association" prénomée "Un p'tit air de Mya", devait venir en aide à leur fillette, atteinte, selon eux, d'une maladie orpheline, la sténose trachéale congénitale.

Alors si vous souhaitez faire don de votre argent en soutenant une cause solidaire, assurez-vous bien de l'existence de l'association et du projet qu'elle porte.

Arnaque à la consommation d'énergie

Un SMS d'arnaque **lié à la consommation d'énergie** circule actuellement en France. Les escrocs usurpent l'identité d'une région, majoritairement les Hauts-de-France, vous informant qu'elle "vous permet **d'économiser plus de 70% sur la consommation énergétique**". Vous êtes alors redirigé vers un lien, **qui vole en réalité vos données personnelles.**

Arnaque à la vignette Crit'Air

C'est un classique de l'année 2022, qui ne s'arrêtera sûrement pas en 2023. **L'arnaque à la vignette Crit'Air r**epose sur un SMS envoyé aux automobilistes, leur demandant d'acheter le papier pour pouvoir circuler **dans les zones à faibles émissions**. Ils sont redirigés vers un site rappelant celui du gouvernement, mais il s'agit en réalité d'une arnaque. Pour être sûr de ne pas vous faire avoir, pensez à regarder le prix car **le prix de la vignette en France est de 3,67 euros frais de port inclus.** Au-dessus, passez votre chemin !

Arnaque à l'urgence familiale

Depuis le début du mois de décembre, de nombreux Français reçoivent le message d'un proche qui aurait cassé son téléphone portable, puis **un second SMS leur demandant d'envoyer de l'argent en urgences.** Avant de vous exécuter, vérifiez que le proche en question est bien dans cette situation et vous comprendrez rapidement qu'il s'agit d'une arnaque.

Extrait d'une publication ancienne de Michel Marrer

La sécurité

Dans les années 80, on ne parlait pas de **cybercriminalité**, mais évoquions les **risques**, le **terrorisme(1)** et les **bombes informatiques(1)** pour les décennies à venir, et à l'époque, la micro-informatique et internet n'étaient pas encore passés dans le domaine public.

Plus de 30 ans après……

Le terrorisme, les bombes informatiques sont là. ….à travers les réseaux sont plus que réaliste, ….menaces sur les infrastructures nationales (électricité, nucléaire, distribution d'eau, hôpitaux, transports, l'état, les collectivités locales…) sont bien réelles – des attaques '**terroristes**' de ce type sont prévisibles dans **les 5 à 10 ans qui viennent.**

A travers internet, les réseaux sociaux, les portables, les tablettes numériques, mais aussi par l'incompétence de certains informaticiens….. la **cybercriminalité** tisse sa 'toile'. Aujourd'hui nous pouvons dire qu'à l'horizon **2025** les possibilités de conflits à venir seront + ou – liées à l'informatique.

Les guerres à venir ce sont celles-là, aussi dangereuses et dévastatrices que les guerres 'conventionnelles'. Les budgets alloués par les Etats pour tenter de s'en prémunir vont se chiffrer en centaines de millions d'euros, plusieurs milliards pour certains.

Les difficultés que nous rencontrions il y a près de 30 ans sont toujours là ! nous avons beau dire aux chefs d'entreprises que les risques d'espionnage industriels sont là et n'ont jamais été aussi grands (cela fait des années qu'on le martèle), ils écoutent soit, et clament qu'il est indispensable de se protéger ! mais dans le même temps continuent allègrement à sabrer dans les budgets sécuritaires.

Et que dire des actionnaires des entreprises du CAC 40 qui auraient sur ce sujet leur mot à dire, mais comme ces derniers sont souvent aussi eux-mêmes chefs d'entreprises, ils ont pour la plupart la même attitude. Seuls ceux qui se sont fait pirater se sentent concernés.

De vraies passoires, voilà ce que pensaient en **2015** certains experts des entreprises Françaises.

Mais ne considérons pas la seule responsabilité des chefs d'entreprises.

Certains sont parfois mal secondés par les informaticiens faisant partie de l'entreprise ou extérieurs, plus soucieux des performances techniques de leurs systèmes (partie visible) que de l'aspect sécuritaire de l'entreprise qui demande, outre les compétences purement techniques : sens de l'organisation, méthode, rigueur, sens du dialogue, de la communication et de la formation.

Les systèmes de sécurité actuels sont conçus (en imageant) comme un réseau de barbelés autour d'une résidence….parfois difficile d'entrer, mais une fois à l'intérieur !!!!

Extrait d'une publication ancienne de Michel Marrer

La différence avec un ordinateur, c'est que les barbelés (outils de protection) sont à l'intérieur et que les portes sont grandes ouvertes à travers les réseaux.

L'éventuelle émergence des ordinateurs de type quantique va, comme vu plus haut, casser tout les codes de protection connus. Alors, que faire ?

Les systèmes de protection d'accès ne règlent qu'une faible partie des problèmes liés à la sécurité. En effet, comme nous l'avons vu plus haut tout est maintenant connecté sur l'extérieur.

Ca n'est pas être alarmiste que d'être conscient. La technologie évolue, les hackers s'adaptent et ont très souvent '**un coup d'avance'**. Il n'y a pas qu'eux, il y a aussi tout ces grands groupes qui proposent le « Cloud » pour sauvegarder vos données personnelles, les réseaux sociaux, les fournisseurs d'accès, les fournisseurs d'outils en ligne…… tout ce petit monde engrange des tonnes d'informations (volontairement ou à votre insu) et en conserve la maîtrise –

il faut souligner aussi que tous grands qu'ils puissent-être, ils ne sont pas à l'abri des pirates (hackers). C'est le serpent qui se mord la queue.

Tous systèmes aussi pointu soit-il a et aura toujours ses failles, la sécurité à 100% n'existe pas.

La seule chose que l'on puisse faire, c'est de tenter de limiter la « casse » en respectant quelques règles élémentaires comme déjà citées, mais surtout en **étant vigilant quant à l'utilisation de nos ordinateurs**, **tablettes, smartphones, cartes de crédit, etc…**

Comme nombre d'inventions avant elles, la mécanographie puis l'informatique ont fait faire un bond extraordinaire à nos sociétés depuis le début des années 60, mais comme dans toutes les avancées, chaque médaille a son revers et génère à un moment donné d'autres problèmes, et les exemples sont nombreux…- Electricité, énergie nucléaire, moteur à explosion, automobile, médecine, médicaments, chirurgie, vieillissement, démographie, eau, pollution,……

L'informatique n'échappe pas à la règle et risque de devenir notre pire cauchemar. Nos sociétés vont promettre monts et merveilles en matière de protection et de surveillance, à travers lois, décrets, etc… , mais ne feront qu'ajouter des textes à l'arsenal législatif déjà existant sans pour autant solutionner.

La cybercriminalité est là. …. menaces sur les infrastructures nationales (**électricité, nucléaire, distribution d'eau, hôpitaux, transports, l'état, les collectivités locales…**) sont bien réelles –

L'exemple (9 avril 2015) du piratage **de TV5** monde étaie malheureusement nos propos. Depuis le début de **l'année 2015 plus de 1500 attaques** ont été recensées visant des sites peu protégés**. L'Ansii (**Agence nationale se la sécurité des systèmes) dispense tous les conseils pour se protéger – ces conseils sont-ils suivis ? on peut en douter !

Le seul et unique rempart c'est l'utilisateur bien informé

Il y a eu les guerres de tranchées, sur mer, dans les airs…… aujourd'hui c'est le numérique qui est devenu un espace de combat et de guerre. En face de la **cybercriminalité et des cyberterroristes, la cyberdéfense des infrastructures nationales** doit-être une priorité.

Il n'y a pas de solution miracle ! la protection passe avant tout par la prévention**. LA SOLUTION**, certains services de renseignements étrangers l'on trouvé……. **(papier, crayon, bonne vieille machine à écrire)** pour communiquer sur des informations vitales et stratégiques.

Dans certaines circonstances, le retour en arrière est parfois nécessaire avant de trouver les solutions qui s'imposent.