CENTENAIRE DE LA SOCIÉTÉ DES MEMBRES DE LA LÉGION D'HONNEUR
100 ANS AU CŒUR DE LA NATION

Proposé par le CA du Vaucluse

SMLH
SOCIETE DES MEMBRES DE LA LEGION D'HONNEUR
SECTION VAUCLUSE

ARNAQUES SUR INTERNET
ENTREPRENDRE DE LES RECONNAITRE, SE PROTEGER ET SI POSSIBLE REAGIR

L'imagination des escrocs est malheureusement sans limite. On trouve de tout sur internet, de la fausse photo de profil sur « une application de rencontres » (*pas bien méchant si cela se limite à cela*) - au faux site créé pour **récupérer les identifiants bancaires**, ce qui est bien plus grave. Quelques grandes dispositions sont cependant à apprécier.

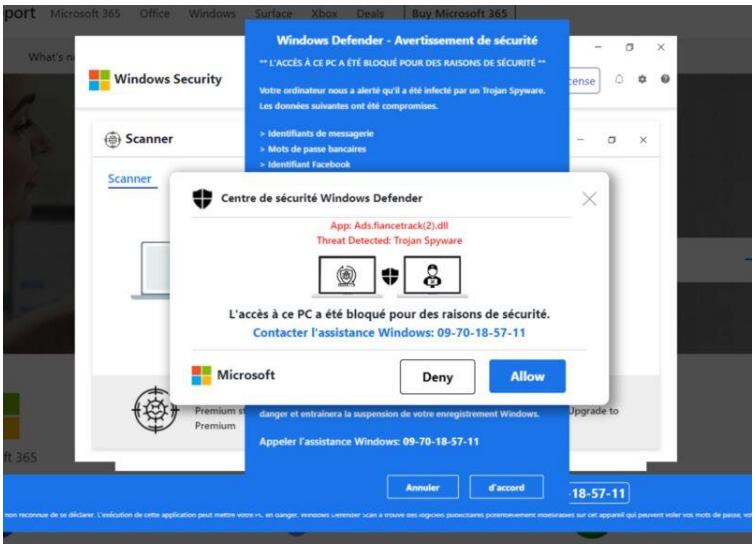
Le phishing ou l'hameçonnage

Très fréquent, le phishing consiste à envoyer un message ressemblant à celui que l'on peut recevoir d'un site reconnu et fiable (site d'e-commerce, banque, organisme gouvernemental, etc.). Le but recherché est de vous amener à communiquer des infos confidentielles (mot de passe, numéro de carte bancaire, etc.) pour les récupérer. Les e-mails de phishing prennent la forme de véritables e-mails. Ils peuvent même apparaitre comme provenant d'une entreprise bien connue et reconnue par vous -même pour abuser de votre confiance.

- Regardez avec grande attention l'adresse électronique de l'expéditeur et le lien avec le contenu de l'e-mail et prenez vos distances en cas de doute.
- Contactez de toute urgence votre banque pour vous opposer à toute utilisation frauduleuse de votre carte. Si vous avez divulgué d'autres informations comme des mots de passe notamment, changez-les aussi. Le faire aussi vite que possible, car dans cette situation le temps est un facteur déterminant pour limiter la casse.

Le faux support informatique

Très pernicieuse, cette technique vise plus particulièrement un public peu à l'aise avec l'informatique. Lorsque vous travaillez sur votre ordinateur tout à coup s'affiche une alerte très anxiogène qui vous annonce que ce dernier est « vérolé » et qu'il faut de toute urgence composer un numéro de téléphone, souvent surtaxé. Cette alerte est parfois accompagnée d'une alarme sonore, histoire d'inquiéter encore davantage. La personne qui répond au téléphone travaille soi-disant au support informatique (certains se disent même mandatés par Microsoft !) et vous propose de prendre la main sur votre ordinateur pour vous aider à régler le problème. Si vous acceptez, vous risquez d'être facturé d'un montant pouvant aller jusqu'à plusieurs centaines d'euros, et **vos données confidentielles risquent d'être dangereusement siphonnées**.



- Au cas où : commencez par le plus urgent, prévenir votre banque et changez les mots de passe les plus urgents (comptes bancaires, messageries personnelles et professionnelles, principaux sites marchands utilisés, administrations, etc.). Ensuite, vous faire aider si besoin pour nettoyer votre ordinateur. Se rapprocher d'un commissariat ou de la gendarmerie pour signaler l'escroquerie, cela pourra servir dans le cas d'une éventuelle usurpation d'identité.

Le chantage à la webcam :

Cela peut arriver que des arnaqueurs prétendent avoir des vidéos de vous en train de regarder des films *coquins*. Ils vont vous faire chanter et demander de l'argent pour ne pas divulguer ces soi-disant vidéos. En réalité, c'est quasi impossible « de hacker une webcam ».

- Ne jamais ouvrir et encore moins répondre au mail, il ne faut surtout pas donner une quelconque suite.

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

- L'Assurance maladie ne demande jamais d'informations pour envoyer votre nouvelle carte vitale au contraire elle envoie couramment des messages de prévention afin que les cibles de ces faux SMS et mails soient particulièrement prudentes.

Le drop shipping

Le drop shipping est une pratique commerciale qui se développe de plus en plus sur Internet, notamment chez les influenceurs et via les réseaux sociaux. Il s'agit d'une technique utilisée par des sites internet qui proposent des produits déjà en vente chez d'autres fournisseurs et qui gonflent artificiellement le prix afin d'empocher une jolie commission au passage. "Par exemple, un influenceur va nous promettre 50% sur une montre si on l'achète sur telle boutique en ligne.

- On se rend compte par la suite que cette boutique n'est qu'un intermédiaire avec le grossiste et qu'elle a obtenu une commission énorme sur notre achat.

L'arnaque "à la nigériane"

Ainsi appelée parce qu'elle venait à l'origine de ce pays d'Afrique de l'Ouest, elle peut aujourd'hui surgir de n'importe quel coin du globe et se déroule selon un plan bien rodé : un pseudo-prince, ministre ou autre fils de bonne famille, souvent africain, cherche à faire sortir clandestinement une très grosse somme d'argent de son pays mais ne peut le faire lui-même, pour x raisons techniques. Il compte donc sur vous et il a bien entendu besoin de vos informations bancaires pour pouvoir virer l'argent. Une variante consiste à vous solliciter pour que vous envoyiez une somme donnée pour débloquer la situation et lui donner accès au pactole, dont il vous reversera une part substantielle.

- Autant dire que dans le premier cas vos comptes seront vidés et que dans le deuxième vous ne reverrez jamais votre argent !

Les faux organismes de charité

Les escrocs n'ont hélas pas de morale et n'hésitent pas à exploiter votre générosité pour vous extorquer de l'argent. On voit ainsi souvent fleurir de faux organismes ou associations après les catastrophes humanitaires. Surfant sur votre empathie et votre compassion après avoir vu des images déchirantes à la télévision ou sur les réseaux, ils touchent une corde sensible et vous proposent de participer à l'effort de reconstruction ou d'aider à acheminer des vivres et vêtements via un don.

- Attention donc aux faux sites et autres cagnottes fantoches.

Les abonnements cachés et produits à l'"essai"

Phénomène qui augmente avec l'émergence des réseaux sociaux. On vous propose de découvrir un produit, une gamme de produits ou un service. Avec un prix "découverte" souvent très alléchant. Vous vous dites que c'est une bonne affaire et un moyen économique de tester le produit ou le service.

- Sauf que vous vous apercevez plus tard ou trop tard que vous avez souscrit à un abonnement au prix fort et que votre compte bancaire est prélevé chaque mois d'une somme non négligeable.

- La DGCCRF (Direction générale de la concurrence, de la consommation et de la répression des fraudes) conseille de demander à la société concernée la résiliation immédiate de l'abonnement et par ailleurs de faire opposition aux prélèvements auprès de votre banque. Si vous avez payé par carte bancaire, vérifiez que vous ne bénéficiez pas d'une couverture incluse pour ce genre de mésaventures. Pour faire simple, sous certaines conditions, vous pouvez obtenir le re-crédit des frais déjà engagés en cas de fraude ou de non-respect avéré des clauses.

Les "intermédiaires" administratifs

Ce genre d'arnaque existe par exemple avec l'ESTA (autorisation d'entrée aux Etats-Unis). Un nombre croissant d'interlocuteurs peu scrupuleux jouent ainsi sur la méconnaissance de l'internaute pour tout ce qui est démarches administratives et font payer au prix fort un service qu'ils font passer pour officiel.

- Certains rendent même payant un service qui est totalement gratuit sur le site gouvernemental.

Les mules financières ou les arnaques à investissement, loteries etc. :

Lorsqu'une personne vous contacte en ligne et vous promet une importante somme d'argent pour pouvoir utiliser votre compte en banque, vous devenez ce qu'on appelle une "mule financière". Cette technique est souvent utilisée par les criminels qui souhaitent blanchir de l'argent volé. L'arnaqueur va gagner notre sympathie et notre confiance, souvent via des sites ou applications de rencontres. Un lien va commencer à se créer sur le web et petit à petit, nous nous faisons arnaquer sans vraiment nous en rendre compte».

De même on vous contacte pour vous parler de fausses œuvres caritatives, de loteries, ou des fameux investissements où "on peut gagner jusqu'à 200% de rentabilité" !

Les seniors sont souvent les cibles privilégiées de ce genre d'arnaques.

- Le seul recours sera de signaler l'abus au site concerné quand c'est possible et de porter plainte en cas d'escroquerie. Les chances de récupérer les sommes perdues restent faibles et dépendront du site. Certains réseaux sont parfois démantelés, mais pour ce qui est du recouvrement des fonds, c'est une toute autre histoire.

Les pornbots

"Les pornbots sont ces robots ou des faux comptes qui existent sur Instagram. Ils vous suivent, ils publient des messages bizarres en dessous de vos publications et ils vous demandent ensuite de cliquer sur des liens douteux.

- Ne pas le faire car la menace d'être arnaqué est importante (demande de numéro de carte bancaire ou adresse e-mail et donc risque de problèmes.)

- **Les faux sites web**

Ils utilisent des adresses quasi identiques aux magasins en ligne bien connus. Ils usurpent les noms de marques célèbres puis disparaissent du paysage pour réapparaître plus tard sous une autre dénomination.

- Il est fort probable que cela soit une tentative d'arnaque. Les escroqueries sont extrêmement fréquentes en ce moment et prennent différentes formes.

Arnaque à l'indemnité inflation

La caisse nationale d'allocation familiale (Cnaf) alertait récemment 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.

- Cependant, l'indemnité inflation est versée directement par l'organisme dont vous dépendez : votre employeur pour les salariés, les Urssaf pour les entrepreneurs, Pôle emploi pour les chômeurs ou encore les caisses de retraite pour les retraités. Comme pour le chèque énergie versé en décembre 2021, aucune information personnelle ne sera demandée par mail.

Faux conseiller bancaire

Au début du mois de février, 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.

- Les arnaqueurs "sont en capacité de passer des appels en faisant en sorte que le numéro de l'appelant qui apparaît ne soit pas celui de la ligne téléphonique utilisée" : très grande vigilance

Arnaque à la rénovation énergétique

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. 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

Le coupon PCS ou carte PCS est une carte bancaire prépayée (Prepaid Cash Service Card en anglais). Usurper l’identité des forces de l’ordre semble être une stratégie privilégiée par les escrocs. 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 par exemple sur des personnes des pays de l'Est. Les escrocs demandent alors de l'aide à leurs victimes, en leur demandant de leur transmettre des coupons PCS qui serviront d'appâts dans leur enquête.

- Si vous recevez un appel de policiers qui vous demandent ce service, gardez en tête que la police se déplace toujours sur le terrain pour enquêter. N’hésitez donc pas à contacter votre commissariat local si vous avez le moindre doute. Lorsqu’il s’agit d’une somme conséquente, il est également possible que votre buraliste fasse de la prévention, en vous demandant si vous connaissez bien votre interlocuteur ou si vous maitrisez bien le système de paiement du coupon PCS.
- De manière générale, lorsque vous êtes intéressés par une annonce sur internet et que celle-ci peut uniquement se régler en carte prépayée, méfiez-vous et rendez-vous sur cybermalveillance.gouv.fr, car il s’agit probablement d’une tentative d’arnaque.

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).

- Pour détecter la supercherie bien vérifier l'adresse de l'émetteur, ainsi que l'orthographe du texte dans le document. Si l’administration fiscale doit un jour vous rembourser une somme quelconque, elle ne demandera jamais au bénéficiaire de transmettre des données personnelles telles que des coordonnées bancaires.

L’arnaque au Compte personnel de formation (CPF)

Le Compte personnel de Formation (CPF) permet à toute personne active d’acquérir des droits à la formation tout au long de sa vie professionnelle. Généralement, ces tentatives d’escroquerie débutent par un coup de téléphone, un SMS ou un mail d’une personne prétextant travailler pour “Mon Compte Formation”, un organisme de formation ou bien encore un organisme public comme la Caisse des dépôts ou le ministère du Travail. Les escrocs cherchent ainsi à obtenir le numéro de sécurité sociale (quand ils ne le connaissent pas déjà) ou le mot de passe de leur victime pour accéder à leur compte CPF.

- Ne jamais communiquer vos informations personnelles et de n'autoriser personne à créer un compte à votre place. Bon à savoir : la Caisse des dépôts et le ministère du Travail ne contactent jamais directement les utilisateurs pour leur rappeler d'utiliser leurs droits CPF. Si vous avez transmis le mot de passe de votre compte personnel de formation à une personne inconnue, changez-le immédiatement.

Comment tenter d'éviter les pièges

Il existe bien d'autres méthodes pour nous tromper sur le net, et il s'en crée tous les jours de nouvelles, impossible de toutes les recenser ici : par contre quelques conseils pour se protéger :

- **N'envoyer jamais vos informations confidentielles** (numéros de carte bancaire, mots de passe, etc.) en réponse à un mail.
  S'il s'agit de votre banque, pourquoi vous demanderait-elle des numéros de carte alors que c'est elle qui vous les a envoyés ? De même, un service client n'a jamais besoin de votre mot de passe pour accéder à votre compte, pas plus d'ailleurs qu'un organisme public. Et un mot doit tout de suite vous alerter, c'est "**Urgent**". Sciemment utilisé pour vous alarmer, il doit au contraire vous inciter à vous poser et à réfléchir dès qu'il est utilisé dans un mail.
- **Prendre le temps de vérifier le sérieux de l'organisme** qui sollicite un don.
  Un simple passage par le net suffit souvent à obtenir de nombreuses informations. Les avis d'autres donateurs devraient vous aider à vous faire une opinion. Et à contrario, s'il s'agit d'une arnaque, il est difficile de le cacher longtemps sur la toile. Les sites de ces organismes bidons trahissent souvent un certain amateurisme, sur la forme et sur le fond. Des erreurs de syntaxe et des approximations doivent vous alerter.
- **Prendre le temps de lire les conditions contractuelles**.
  Concernant l'arnaque aux faux produits d'essai, la mention d'un abonnement est bien présente dans les conditions de vente, mais soigneusement noyée dans les informations pour que vous passiez à côté.
- En cas d'infection d'un ordinateur, **ne cédez surtout pas à la panique**.
  La plupart du temps, il s'agit d'une arnaque très simple à contourner en éteignant votre ordinateur et en le relançant en mode sans échec pour le nettoyer. Si vous ne pouvez pas l'éteindre, essayez la combinaison de touches "CTRL + ALT + SUPPR" pour fermer la session. Quoi qu'il arrive, **n'acceptez jamais la prise en main à distance de votre ordinateur par un support que vous n'avez pas sollicité**.
- Pour toute démarche administrative, **passez par les sites officiels**, jamais par des intermédiaires.
- **Privilégiez autant que possible les enseignes et organismes reconnus**, ayant pignon sur rue.
  Les sites exotiques aux conditions de ventes floues ou mal traduites sont à fuir comme la peste, même s'ils proposent des tarifs imbattables. Et il ne faut pas hésiter à consulter les avis des autres utilisateurs, souvent ils vous éviteront les mauvaises surprises. Sans compter que sur le net les nouvelles vont vite, si d'autres se sont fait avoir, vous en trouverez surement les échos en tapant "*avis + nom de la société ou marque ou organisme*" dans le moteur de recherche.
- N'hésitez pas, en cas de doute, à **consulter le site de la répression des fraudes (DGCCRF).**
  Consultable gratuitement le site recense de nombres types de fraudes et arnaques visant les particuliers mais aussi les professionnels, et conseille sur les moyens de les identifier et les noms d'organismes vers lesquels se tourner si besoin.
- **Gardez l'ordinateur ou le terminal à jour**
  C'est surtout important pour ce qui concerne la suite antivirus, qui inclut d'ailleurs souvent un anti-phishing. Idem pour le navigateur internet, ils proposent tous une fonction de protection contre les sites malveillants.
- **Attention aux "bons plans" gratuits**.
  Les sites de téléchargement -ou de streaming- illégaux sont par exemple connus pour être de véritables nids à infections. C'est notamment la porte d'entrée privilégiée des arnaques au faux support téléphonique. Attention aussi aux logiciels gratuits et « crackés » proposés sur certaines plateformes. Le coût de la gratuité peut alors devenir exorbitant !

T**out ce qui brille n'est pas de l'or.** Une offre trop avantageuse doit immédiatement inciter à la prudence, en particulier s'il est demandé de verser d'abord de l'argent pour en recevoir

POUR AUTANT UTILISER INTERNET ET LE WEB RESTE TRES OPÉRANT AVEC D' INÉVITABLES PRECAUTIONS