Guide de prévention contre les arnaques

Avec la crise du Covid 19, les entreprises et les consommateurs subissent des manœuvres frauduleuses de tous ordres et il est important d'être vigilant pour déjouer les arnaques potentielles. À cette fin, les services de l'État et les autorités de contrôle s'associent et proposent des fiches préventives d'identification des principales fraudes.
Un guide avec des fiches préventives d'identification des principales fraudes a été édité et vous pouvez le retrouver avec le lien https://www.douane.gouv.fr/sites/default/files/2021-03/25/guide-de-prevention-contre-les-arnaques-sur-internet.pdf

Voici les principales menaces existantes et en bas de page les sites importants à connaitre :

Les achats sur internet :

Il faut vérifier l'identité du vendeur. Choisir un site français ou européen de préférence (l'URL**.fr** ne signifie pas forcément que le site est français). Vérifier sa e-réputation en associant le nom du site avec le mot arnaque. Être attentif au descriptif des produits et au marketing agressif.

Besoin de gel hydroalcoolique :

Choisir un gel de bonne qualité (norme NF RN 14476) à base d'alcool avec un % supérieur à 60% (alcool éthylique ou éthanol ou propylique ou isopropylique).

Epargne et crédits :

Attention aux recrudescences des arnaques aux placements, aux crédits et aux assurances trouvées sur internet ou par contact téléphonique ou sur le web.
Consultez les listes noires et tableau des alertes sur les sites internet **Assurance Banque Épargne Info Service (ABEIS) et l'Autorité des marchés financiers (AMF).**

Faux ordres de virements :

Se méfier des propositions commerciales « urgente ». Ne pas communiquer d'informations susceptibles d'aider les escrocs (mots de passe, IBAN…). Modifier régulièrement ses mots de passe, ne pas mettre le même partout et le rendre complexe. Appeler sa banque rapidement en cas de doute ainsi que la gendarmerie et la police avec un maximum d'éléments.

Usurpations d'identité :

Perte d'un papier d'identité, justificatif de domicile ou simple photocopie mis dans la poubelle, site web, contact sur un réseau social ou simple sms, tout est bon pour les escrocs pour récupérer votre identité et vous mettre dans des situations parfois dramatiques. Les faux messages par mail provenant soi-disant de l'état (aides, attestations de déplacement, remboursement d'impôts …) ou d'autres institutions sont très fréquents. Ces usurpations sont principalement commises par phishing (hameçonnage) par un faux site web ou un faux profil sur un réseau social.
Ne JAMAIS ouvrir un sms, un courriel ou un profil inconnu. N'oubliez pas que les institutions publiques ou les autorités de contrôle ne sollicitent JAMAIS la communication d'informations personnelles ou le versement d'argent par courriel ou téléphone.

Faux sites administratifs :

De nombreuses démarches administratives sont proposées gratuitement sur des sites officiels mais il n'est pas interdit à des professionnels de proposer ces prestations en contrepartie d'un paiement mais à condition qu'ils respectent des règles précises (identité, tarifs, délais 14 jours de rétractation …).
Le site officiel du gouvernement : www.service-public.fr.
Pour consulter le sérieux d'une société qui propose un service : https://www.europe-consommateurs.eu/index.html.

Hameçonnage ou *phishing* :

Technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (mots de passe…) et/ou bancaire en se faisant passer pour une personne de confiance (votre banquier, services médicaux sociaux, administration …).
Soyez attentif aux fautes d'orthographe, aux expressions bizarres, aux liens avec une lettre en plus ou en moins … . Toute demande étrange est à éviter en contactant votre expéditeur par un autre canal.
Un antivirus à jour, un logiciel bloqueur de publicités peuvent suffire. Ne pas ouvrir les pièces jointes, supprimer le message ainsi que la corbeille.

Appels frauduleux aux dons :

Vérifiez que l'entité qui fait un appel aux dons est autorisée à le faire en consultant le site de l'ORIAS **www.orias.fr** qui est registre du secteur financier ou qu'il ne fait pas partie de la liste noire sur le site ABEIS **www.abe-infoservice.fr.**

Fraudes aux fausses réparations informatiques :

A l'occasion d'une navigation sur internet, un message de sécurité anxiogène sous une apparence légitime apparait dans une fenêtre prétendant la présence d'un maliciel (logiciel malveillant) ou d'un problème technique, un service de support technique devant être contacté pour remédier au problème.
Mettre à jour votre antivirus, activez votre pare-feu, évitez les sites non surs ou illicites ou pornographiques. Si vous êtes bloqués, redémarrez votre ordinateur. Désinstallez toute nouvelle application suspecte. Si un faux technicien contrôle votre machine, désinstallez le programme de gestion à distance et changez vos mots de passe. Sans possibilité d'action, faire appel à un prestataire référencé sur www.cybermalveillance.gouv.fr.

Vol de coordonnées bancaires :

Réaliser vos achats uniquement sur des sites de confiance signalés par le logo « cadenas » et dont l'adresse commence par « https ». Ne pas enregistrer son numéro de carte bancaire sur le site commerçant ou sur l'ordinateur. Au distributeur de billets, bien se cacher et ne pas se laisser distraire.

Rançongiciels (logiciels malveillants dans l'ordi) :

Demander une rançon pour libérer les données cryptées en échange d'une clé ou d'un mot de passe pour les déchiffrer.
Débrancher la machine d'internet, isolez les supports touchés par ce piratage, ne pas payer et déposez plainte. Vous pouvez trouver quelques clés et outils de déchiffrement sur le site **:** **nomoreransom.org/fr/index.4html.**

Pour TOUTES les arnaques 4 sites à connaitre :

Vous êtes victime d'une tentative d'escroquerie, la signaler sur la plateforme **PHAROS** accessible sur le site **www.internet-signalement.gouv.fr**
En cas de doute sérieux sur un site administratif, vous pouvez le signaler à la ***DGCCRF*** **https://www.economie.gouv.fr/dgccrf/contacter-dgccrf**
Vous êtes victime d'une escroquerie, vous pouvez initier une plainte sur internet :
https://www.pre-plainte-en-ligne.gouv.fr/ ou Info Escroqueries au 08 11 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0,06€/minute si par mobile) du lundi au vendredi de 9h à 18h.
Pour tout acte de cyber malveillance rendez-vous sur **cybermalveillance.gouv.fr**.