



ME PRÉMUNIR CONTRE LES ARNAQUES EN LIGNE



Lieu de sociabilité et de partage de connaissances, internet est également devenu l'espace de nos démarches administratives et une grande place de marché.

Nous y faisons circuler de nombreuses informations personnelles et des documents qui ne doivent pas tomber entre des mains malintentionnées. En particulier, les messageries privées et les réseaux sociaux sont des espaces de prédation privilégiés par les escrocs 2.0. Apprenons quelques gestes et réflexes simples pour se prémunir contre la plupart des arnaques en ligne, repérer les spams, "phishing*" et autres messages frauduleux.

Les principaux types d'arnaques :

• Les faux messages institutionnels

Il n'est pas rare de recevoir un e-mail ou un sms imitant la demande d'une institution de confiance (banque ou opérateur de service public) dont l'objectif est de vous faire cliquer sur un lien frauduleux ou demander des informations de connexion permettant d'usurper ensuite votre identité.

Rappelez-vous qu'il ne vous sera jamais demandé par un acteur institutionnel de fournir vos identifiants, ni par téléphone, ni par e-mail, mais toujours dans un espace sécurisé.

Exemple de message frauduleux. Le numéro de téléphone utilisé par les fraudeurs (+337000008735314) est un indice efficace pour déceler les fraudes.



• Les demandes d'aides suspectes

Les réseaux sociaux sont un terrain de chasse privilégié pour des escrocs opérant avec de faux profils (utilisant le nom et l'image d'une personne fictive) pour entrer en contact et en empathie avec des victimes potentielles, en utilisant parfois de véritables tactiques de séduction.

Si vous faites l'expérience de rencontrer de nouvelles personnes sur internet, nous vous déconseillons fortement de donner suite à des demandes d'aide qui impliquent des transactions financières ou l'envoi de documents personnels, même si la personne qui vous écrit semble en difficulté.

Par ailleurs, nous vous déconseillons réellement d'envoyer des photos intimes à des inconnus, celles-ci pourraient être utilisées pour du chantage.



ME PRÉMUNIR CONTRE LES ARNAQUES EN LIGNE



Lieu de sociabilité et de partage de connaissances, internet est également devenu l'espace de nos démarches administratives et une grande place de marché.

• Les demandes d'aide financière urgente de vos contacts

Ces mêmes demandes peuvent provenir de vos proches ou connaissances par mail ou par messages privés sur les réseaux sociaux. Par exemple, vous recevez un message inquiétant d'une amie dont vous n'avez pas eu de nouvelles depuis plusieurs mois. Cette dernière vous demande un virement urgent, car elle est en voyage et qu'on lui a volé son portefeuille.

Ce message est très certainement une arnaque. Le compte mail de votre amie a été piraté et ainsi, son identité a été usurpée par un escroc. Par conséquent, au moindre doute, vérifiez si l'information du message est vraie : contactez votre amie, ou appelez ses proches pour connaître la vérité. Si le message contient des liens, ne cliquez pas dessus. N'ouvrez pas les pièces jointes. Ne donnez aucune information personnelle par retour de mail.

Soyez vigilant : si l'un de vos proches ne répond pas de la même manière qu'habituellement, il se peut qu'il ait été piraté. Le message peut être moins suspect que l'exemple donné précédemment.

• La vente de contrefaçons ou de produits de mauvaise qualité

De nombreuses personnes peu scrupuleuses se font une spécialité de vendre à des prix défilant toute concurrence des produits qui semblent de bonne qualité sur les photos, sous couvert de promotions très importantes. Il n'est pas rare que ces produits soient en fait des imitations grossières ou encore des produits de très mauvaise qualité.

Ces ventes ne sont pas illégales, mais ne sont pas honnêtes pour autant et vous en serez déçus. Cette pratique s'appelle le "dropshipping", elle consiste à revendre avec une marge très importante des produits de mauvaise qualité achetés sur des sites spécialisés. En cas de doute, il est possible de consulter le site <https://captaindrop.com/> qui référence les sites de ce type.





ME PRÉMUNIR CONTRE LES ARNAQUES EN LIGNE



Lieu de sociabilité et de partage de connaissances, internet est également devenu l'espace de nos démarches administratives et une grande place de marché.

Les gestes à adopter :

- Il faut regarder l'**expéditeur de l'email** pour voir si l'adresse mail semble louche. Exemples d'adresse mail d'arnaque :
 - De : Colissimo <info2791@knusy.com>
 - Date: ven. 16 févr. 2024 à 13:59
 - Subject: Notification de suivi, le colis a quitté l'entrepôt
 - De : **chrono-poste-express** <LhsnlXzk@kphkspgwp.us>
 - Date: mar. 27 févr. 2024 à 07:30
- Les services administratifs tels qu'impôts, police, banques etc. ne vous enverront JAMAIS de mail pour payer en ligne, vérifier une information, demander vos identifiants, etc.
- Ne JAMAIS partager vos identifiants à qui que ce soit, même vos conseillers personnels en ligne.
- Appelez votre interlocuteur traditionnel avant toute activité demandée par mail ou internet.
- Assurez-vous que l'URL (adresse d'un site ou d'une page internet) du site est correcte et correspond à celle que vous avez l'habitude d'utiliser. Prenez le temps de bien lire et relire l'adresse. Les fraudeurs sont très malins. Les URL des services de l'état finissent par .gouv.fr par exemple.
- Utilisez des favoris pour accéder aux sites Web au lieu de cliquer sur des liens provenant d'e-mails ou de messages. Depuis votre lien habituel, vous pourrez vous connecter à votre espace personnel et retrouver les informations ou actions demandées.
- À noter : Les favoris sont une fonctionnalité du navigateur permettant de sauvegarder une adresse internet et d'y accéder directement via les 'favoris' (étoile).
- Assurez-vous que le site utilise une connexion sécurisée (https://) pour protéger vos informations lors de la transmission.
- Soyez prudent lorsque vous trouvez des liens vers des sites que vous ne connaissez pas, en particulier s'ils sont partagés via des sources non fiables.
- Si le prix d'un article est trop attractif, il s'agit probablement d'une arnaque. Surtout sur des sites que vous ne connaissez pas. Faites une recherche sur un moteur de recherche (Ecosia est très bien) pour trouver des avis sur le site vendeur.
- Si vous n'avez rien commandé, aucune chance pour que Chronopost, DPD ou tout autre livreur ou agence ne vous envoie un mail ou un SMS, notamment pour vous demander de payer quelque chose. Et même si vous avez commandé, ils vous appelleront! Dans tous les cas, ne cliquez pas sur ces mails. Poubelle !

Exemple de mail d'arnaque :

Ne téléchargez pas de fichiers aux noms étranges, sur des sites aux noms étranges. Les fichiers de sources inconnues peuvent contenir des virus qui empoisonnent votre ordinateur et/ou collectent vos données.





ME PRÉMUNIR CONTRE LES ARNAQUES EN LIGNE



Lieu de sociabilité et de partage de connaissances, internet est également devenu l'espace de nos démarches administratives et une grande place de marché.

Les gestes à adopter :

- **Phishing** : Les fraudeurs envoient des e-mails ou des messages qui semblent provenir d'organisations légitimes pour inciter les utilisateurs à divulguer des informations personnelles telles que des mots de passe ou des données financières. Ils vous invitent à cliquer sur un lien qui vous enverra probablement sur un site miroir
- **Site miroir** : Les sites miroirs malveillants sont créés dans le but de tromper les utilisateurs. Ils imitent un site officiel. Ils peuvent être utilisés pour des activités frauduleuses, telles que le phishing. Par exemple, un fraudeur peut créer un site miroir d'une banque populaire, collecter les informations de connexion des utilisateurs et les utiliser à des fins frauduleuses.
- **Spams** : Messages non sollicités, souvent à caractère publicitaire, envoyés en masse via divers canaux de communication en ligne.
- **Dropshipping** : Pratique consistant à vendre un produit sans l'avoir en stock, en le commandant directement sur un site tiers. La plupart des sites de dropshipping font miroiter des bonnes affaires et fournissent des produits de mauvaise qualité.