

Quelques exemples d'arnaques, pour mieux s'en prémunir

Afin de se prémunir des arnaques du numérique, cette fiche a pour objectif de vous donner quelques exemples de types d'attaques qu'on peut recevoir.

Un point important : ce ne sont que des exemples donnés à un moment précis. Il est important de rester prudent, car le type d'arnaques peut évoluer à l'avenir. **Le site cybermalveillance.gouv.fr est une ressource pratique pour rester à jour sur l'actualité des cyberattaques.**

En parallèle, on garde en tête ces **2 éléments** qu'on trouve très souvent dans les arnaques aujourd'hui : **L'urgence, et une notion directe ou indirecte d'argent.** On ne trouve pas toujours ces 2 notions, mais elles sont quand même très souvent utilisées par les arnaqueurs.



Les mails (souvent de phishing) :

Ce sont des mails qui vous informent d'un **problème à régler**. On vous apprend **un souci de livraison** de colis, **d'un remboursement ou d'une dette** avec les impôts, ou Améli etc..

Certains mails vous informent **d'un paiement réalisé**, ou **d'une fraude observée sur votre compte**, et **vous propose d'annuler ce paiement**. Un exemple est *d'un abonnement à Amazon prime pour une somme assez élevée, afin de vous faire cliquer sur le lien pour résilier l'abonnement, alors que vous n'aviez rien réalisé auparavant avec Amazon.*

Deux autres types de mails existent aussi. Les mails de la police, ou de la justice, qui vous informent de crimes, souvent très graves, comme de la pédopornographie, **afin de vous faire répondre/agir pour vous défendre des accusations**. L'autre type de mail est celui qui vous informerait **d'un piratage, ou du risque de perdre ses données en lien avec un cloud**. Ici, la peur s'articule sur la perte de vos données en ligne.



Les SMS :

Par SMS, on trouve souvent des exemples similaires, mais plus courts, que ceux des mails.

Carte Vitale à mettre à jour, amende à payer avant majoration, colis qui ne passe pas dans la boîte aux lettres.

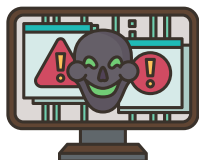
2 autres choses qu'on croise parfois : des **sms de démarchage** (souvent autour de thème de l'énergie, ou d'actualité), et **des messages d'inconnus, parfois aussi par Whatsapp**. Il peut s'agir de véritables inconnus, il arrive qu'une personne vous envoie un message par erreur, mais il peut aussi s'agir **de quelqu'un qui essaye de se faire passer pour un proche**. Souvent **soit coincé à l'étranger, ou à l'hôpital, qui à besoin d'aide financière**.

Les appels intempestifs :

Troisième méthode d'arnaque, les appels. Les appels provenant de **numéros inconnus, appels de démarchage pour des méthodes d'économies d'énergie etc...**

L'élément à surveiller, c'est de vérifier si l'on connaît le numéro ou non et, **si on décroche, de bien faire attention aux infos qu'on donne par téléphone**. Notamment à cause des fuites de données qui ont pu se produire récemment, les malfaiteurs ont parfois accès à certaines infos pour donner un air de légitimité à leur appel.

Voici également différents cas de figures spécifiques qui ne rentrent pas directement dans une des catégories précédente



Sur Internet, les pop-ups et faux support technique :

Attention en ligne à des messages **qui vous informent d'un virus ou d'une panne, avec un numéro de réparation/ d'assistance à appeler**. Il n'y a pas de support technique Windows. Si le message fait du bruit, et qu'il ne se ferme pas normalement, **c'est sans doute un "pop-up" intempestif**, qui essaie de vous mettre la pression. En cas de doute, vous pouvez forcer l'arrêt de l'ordinateur, puis le rallumer.

Les sites de vente entre particuliers :

Attention notamment **aux locations ou à l'achat de voiture ou de biens chers**. Ce sont des situations où l'on peut parfois **vous demander certains papiers non nécessaire, et augmente le risque d'usurpation d'identité**. Si un vendeur vous fait des demandes qui vous font douter, grande méfiance. On garde aussi l'oeil si **les prix semblent trop beau pour être vrai !**

Les types d'arnaques en liens aux sites de rencontre :

Ici, le but est souvent de 2 types. Le premier est semblable au proche qui vous contacte pour demander de l'argent. **La personne va user de la relation établie pour demander un soutien financier**.

Le deuxième cas **relève du chantage, la sextorsion**. Le but est pour l'escroc de convaincre la personne d'envoyer une photo compromettante, généralement grâce à un faux profil. **Une fois la photo partagée, cela sert d'élément de pression sur la personne, pour lui extirper de l'argent, au risque de publier la photo de manière publique**.



Les arnaques "légalement grises" :

Souvent liées aux encadrés "sponsorisé" des recherches en ligne, l'exemple typique est celui de la carte grise. Vous trouverez nombre de site qui propose de faire la démarche, moyennant paiement, alors que celle-ci est normalement gratuite. **Mais comme le service est bien rendu et permis par l'État, cela reste techniquement légal, bien qu'ambivalent, car ces sites profitent du flou qui peut exister sur les démarches en ligne**.

Les arnaques potentielles autour de l'IA :

Petit point de rappel **qu'avec l'IA, certaines arnaques peuvent être perfectionnés**. Usurpation d'identité, dialogue plus réaliste, faux site mieux réalisé etc... On garde toujours l'oeil sur la notion d'urgence et de prudence, qui sont presque toujours présente pour nous faire craquer, IA ou non.



Petit rappel des bonnes pratiques :

Ne pas agir dans l'urgence ! Rester méfiant si l'on nous demande des informations personnelles . Ne pas répondre aux numéros inconnus si possible. Attention dès qu'une notion d'argent est mentionnée. Attention au téléphone, on ne sait pas toujours qui est au bout du fil.