LES BONNES PRATIQUES SUR INTERNET

- avoir un antivirus et un ordinateur à jour.

- ne rien installer (logiciels, programmes, applications) d'origine douteuse.

- ne pas ouvrir les messages suspects, leurs pièces jointes et ne pas cliquer sur les liens qui peuvent s'y trouver.

- penser à faire des sauvegardes régulières sur une clé usb ou un disque dur externe.

- choisir des mots de passe forts (majuscules, minuscules, chiffres, caractères spéciaux) différents pour chaque site.

- rester sur des sites sécurisés.

- si une connaissance demande de l'aide par mail, la contacter par d'autres moyens (téléphone, sms) pour vérifier si elle est réellement dans le besoin (même si elle demande de ne pas le faire).

- ne jamais donner d'argent (coupon PCS, western union, virement bancaire) à des inconnus ou à des personnes rencontrées récemment sur internet.

- faire attention aux messages contenant trop de fautes d'orthographe ou une grammaire approximative.

- toujours se méfier des « frais annexes » (douanes, acheminement coûteux, diverses taxes…) lors de transactions financières avec des particuliers.

- tout ce qui est trop beau pour être vrai est une arnaque !

- **Méfiez vous de tout le monde sur internet et en cas de doute, n'hésitez pas à prendre contact avec la Gendarmerie, même pour obtenir des conseils.**

Informations utiles :

Ministère de l'intérieur

Site Sécurité internet

Site internet ANSSI

En cas de doute composez le 17

Coordonnées de votre brigade locale :

MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Gendarmerie nationale

LES DANGERS D'INTERNET

En 2019, plus de 90 000 victimes d'arnaques sur internet ont été recensées, contre 28 855 en 2018, **soit une augmentation de plus de 210%**. Parmi ces victimes, 90 % sont des particuliers.

On utilise le terme technique de **« cyber-malveillance »** pour regrouper tous les types d'arnaques et d'attaques présentes sur internet.

La plupart du temps, les escrocs dirigent leurs attaques contre un maximum de personnes pour augmenter leurs chances de piéger des victimes.

Le but recherché est de **récupérer des données personnelles ou de l'argent**.

ATTENTION AUX VIRUS INFORMATIQUES !!!

C’est quoi ???
=> un programme informatique malveillant.

Ça sert à quoi ???
=> son objectif est de perturber le fonctionnement normal de mon ordinateur.

Comment ça marche ???
=> il en existe plusieurs types comme le rançongiciel, le cheval de Troie, le logiciel espion… Les virus peuvent s’infiltrer dans mon système informatique quand j’ouvre un message (mail, MMS, chat), une pièce jointe ou quand je clique sur un lien frauduleux.

Quelles conséquences pour moi ???
=> si j’ai un antivirus, il devrait m’alerter 
=> sinon, mon ordinateur va ralentir, se bloquer, des fenêtres ou des messages d’erreur vont s’afficher, mes logiciels ou mes programmes vont se modifier sans raison 

Quel est le but recherché ???
=> prendre le contrôle de mon ordinateur pour en faire un usage frauduleux,
=> m’espionner,
=> me dérober des données personnelles et/ou confidentielles,
=> me faire du chantage pour me demander de l’argent ou une rançon.

Exemple de mail frauduleux :

Quelques conseils lors de la réception des mails :

- vérifier l’adresse mail de l’expéditeur.

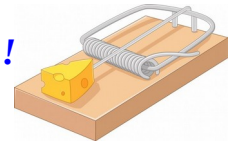
- ne pas paniquer si le mail indique une erreur en votre défaveur, un problème ou une mise à jour nécessaire (*c’est justement le but recherché !!*).

- ne jamais cliquer sur un lien, surtout pour communiquer vos données bancaires (*les impôts, les banques, ERDF, ne vous demanderont jamais vos coordonnées bancaires !!*).

- ne jamais ouvrir les pièces jointes suspectes.

- supprimer définitivement et immédiatement le message une fois identifié comme suspect.

LES PIÈGES À ÉVITER !!!



<u>Les faux mail provenant d’une connaissance...</u>
=> l’escroc se fait passer pour un de vos amis après avoir pris le contrôle de sa boite mail dans le but de vous soutirer de l’argent en faisant croire à une situation de détresse. Lors de l’échange, il vous demandera de n’en parler à personne pour justement éviter de se faire démasquer.

<u>Les faux supports...</u>
=> lors de la visite de certains sites internet, une fenêtre s’ouvre en vous faisant croire que votre ordinateur est infecté et vous invite à appeler un numéro de téléphone pour nettoyer votre machine, moyennant finances.

<u>Les arnaques aux sentiments...</u>
=> régulièrement utilisée sur des sites de rencontres et sur des réseaux sociaux (facebook, Instagram), l’escroc noue des liens avec la victime. Il utilise ensuite cette confiance pour lui demander de l’argent en raison d’un besoin urgent (médical, financier…).

<u>Les chantages à la webcam…</u>
=> l’escroc menace de diffuser des photos ou vidéos prises avec la webcam de la victime à son insu ou avec son accord, si elle refuse de lui donner de l’argent.

<u>Les arnaques provenant de sites « achats-ventes »...</u>
=> 30 à 40 % des annonces sont d’origine frauduleuse !! Il s’agit d’offres alléchantes de ventes, de locations immobilières ou de ventes/dons d’animaux, dans lesquels l’escroc va demander des frais supplémentaires ou un paiement immédiat (alors que le bien proposé n’existe pas).