

## **Protégez vos ordinateurs, smartphones, tablettes, clés usb et vos données.**

Voici quelques informations utiles ou rappels pour se protéger.

En 2020, nous étions 4,5 Milliards d'internautes et 30 Milliards d'objets connectés d'où l'importance de nous protéger.

Voici différentes attaques :

**Le rançongiciel** est un virus qui s'infiltré dans votre système, il chiffre et bloque l'accès à vos données et pour les récupérer on vous demande une rançon.

Ceci se pratique surtout pendant les périodes de fêtes, fin d'année, week-end et en Juillet et Août, il part le plus souvent d'un spam , d'un lien, de pièces jointes, aussi de sites malveillants, clé Usb, publicités.

Même avec un antivirus, nous pouvons être victime d'un rançongiciel

Si vous êtes victime de rançongiciel :

couper tout,  
débrancher le câble ethernet,  
couper la Wifi  
pas de partage de connexion

**Le phishing**, ce sont de faux messages que l'on croit venant d'organismes tels que La Banque Postale, Impots Gouv, CPAM...

Avant d'ouvrir le mail :

- \_ vérifiez l'orthographe du site expéditeur, assurez-vous que celui-ci soit le bon
- \_ soyez méfiant si l'on vous presse ou incite à cliquer sur un lien

Exemple : Vous recevez un mail de votre banque qui vous demande de cliquer sur un lien . Il est conseiller de ne pas cliquer sur celui-ci, mais d'aller sur votre site bancaire et d'agir à partir de celui-ci

**Le FOVI** : Faux Ordres de Virement

C'est une arnaque qui, par persuasion, menaces ou pressions, vise à amener la victime à réaliser un Virement de fonds non planifié.

## ADOPTER LES BONNES PRATIQUES

- \* Il est très important de réaliser **les mises à jours**
- \* Les **mots de passe** doivent comporter au minimum **12 caractères**  
 ( avec majuscules, minuscules, chiffres et caractères spéciaux)
  - \_ Un mot de passe est personnel
  - \_ Ne pas utiliser le même mot de passe plusieurs fois

COMBIEN DE TEMPS POUR CRAQUER VOTRE MOT DE PASSE ?					
NOMBRE DE CARACTÈRES	UNIQUEMENT DES CHIFFRES	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES + CARACTÈRES SPECIAUX
4	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT
6	IMMÉDIAT	IMMÉDIAT	IMMÉDIAT	1 sec	5 sec
8	IMMÉDIAT	5 sec	22 min	1 Heure	9 Heures
10	IMMÉDIAT	58 min	1 mois	7 mois	5 ans
12	45 sec	3 semaines	300 ans	2 000 ans	34 000 ans
14	41 min	51 ans	800 000 ans	9 millions d' années	200 millions d' années

Source : SCSF / Nadine AISSANI

<https://i.pinimg.com/736x/d8/0a/6f/d80a6f379b5d3408534abe60c6b454c4.jpg>

**COMBIEN DE TEMPS POUR CRACKER VOTRE MOT DE PASSE ?**

123454 > moins d'une seconde....

acbd1234 > 16 minutes

Az5Ed4pf4 > 1 mois et 25 jours

**N°a3!&Z@9-2% > 57 000 ans**

<https://www.buzzwebzine.fr/wp-content/uploads/2016/10/cracker-mot-de-passe.png>

- \* Il existe entre autres un gestionnaire de mots de passe : keypass.info
- \* Bien **séparé** l'usage **professionnel et privé**, tel que clé USB
- \***Sauvegarde régulières** de vos données sensibles ou précieuses:
  - au moins 3 exemplaires de vos données
  - \_ 1 donnée originale et 2 sauvegardes sur 2 supports différents
  - \_ stocker la sauvegarde 2 dans un autre emplacement physique : l'externaliser
  - \_ tester régulièrement les sauvegardes et restaurations
- \*Pour envoyer des **fichiers confidentiels, importants, sensibles**, il existe :
  - \_ fromsmash
  - \_ 7- zip
- \* Pour **verrouiller une session** : touche windows + touche L
- \* Ne pas brancher de **clé USB** dont on ne connaît pas la provenance

#### Informations supplémentaires :

Vous pouvez visualiser les menaces informatique en temps réel dans le monde via ce site :  
[cybermap,kaspersky.com](http://cybermap.kaspersky.com)

Voici quelques courtes vidéos sur la sécurité en informatique :

- 1) Film Sécurité Security Social Network E6 I Airbus
- 2) Film sécurité Security USB I Airbus

En souhaitant que ces informations vous aient été utiles .