



Les 10 règles de bases de la sécurité sur internet



Mot de passe



Choisir un mot de passe fort, c'est-à-dire avec :

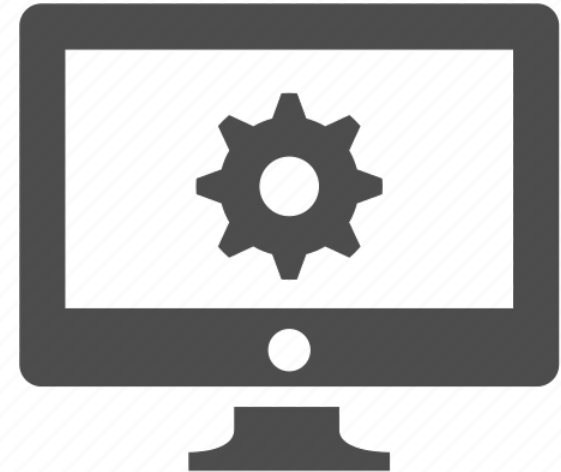
- Au moins une majuscule
- Au moins un chiffre
- Au moins un caractère spécial (@ : / & ! -> *etc*)
- Un minimum de 8 caractères
- Changer régulièrement de mot de passe
- Eviter les mots de passe avec votre nom, votre date de naissance, etc...



Systeme d'exploitation et logiciels à jours

Toujours veiller à la mise à jour du système d'exploitation et des logiciels, **SURTOUT** :

- Antivirus
- Navigateur
- Bureautique
- Mail
- Etc...



Les sauvegardes



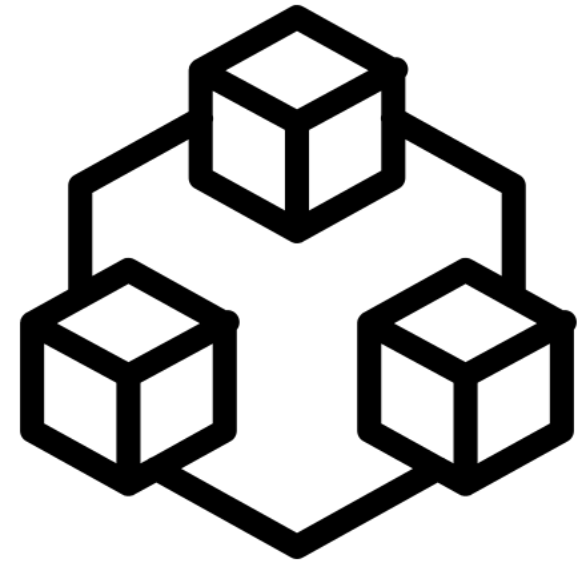
Faire des sauvegardes de vos données **REGULIEREMENT**

Dans le cloud

Et/ou sur un support externe (Disque dur, CD, etc...)

Les modules comme ActiveX et JavaScript

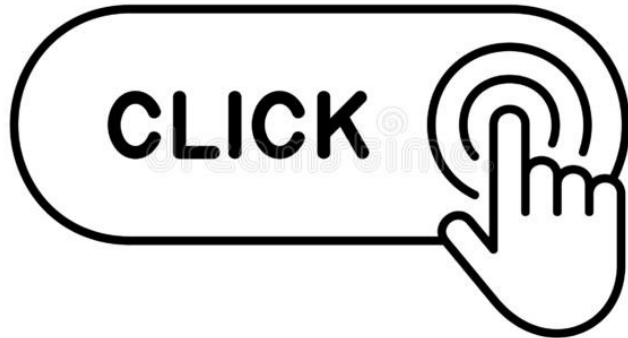
Même si ces modules ont eu leur utilités en leur temps, il faut les désactiver car ils présentent des failles de sécurité très important





CONSEILLER
NUMÉRIQUE
France
services

Ne pas cliquer trop vite sur les liens



Surtout ne pas cliquer trop vite sur les liens des sites internet car certains imitant très bien certains sites ou popup célèbres peuvent vous induire en erreur

Ne jamais utiliser un compte administrateur pour naviguer

Il faut privilégier la navigation sur internet avec un compte utilisateur

Cela permet de limiter le risque de compromission ou d'infection de l'ordinateur

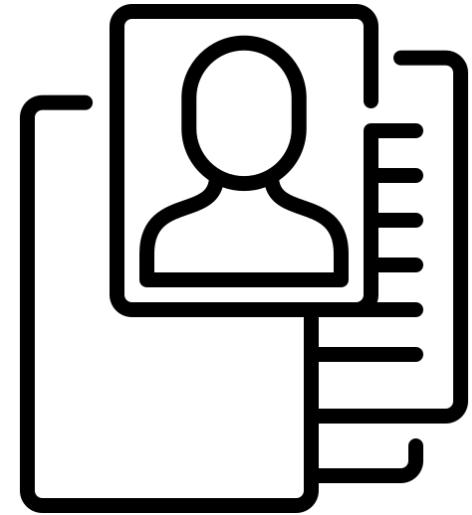


Contrôler la diffusion d'informations personnelles

L'Internet n'est pas le lieu de l'anonymat et les informations que l'on y laisse s'échappent instantanément !

Dans ce contexte, une bonne pratique consiste à ne jamais laisser de données personnelles dans des forums, à ne jamais saisir de coordonnées personnelles et sensibles (comme des coordonnées bancaires) sur des sites qui n'offrent pas toutes les garanties requises

Dans le doute, mieux vaut s'abstenir...



Ne jamais relayer des canulars ou des fakenews

Toujours vérifier la source de l'information que l'on veut partagé

Internet est un formidable outil de connaissance et de savoir mais de nombreux sites diffusent de fausses informations et même parfois de manières virales



Restez prudent, tout le monde sur internet n'est pas forcément votre « ami »

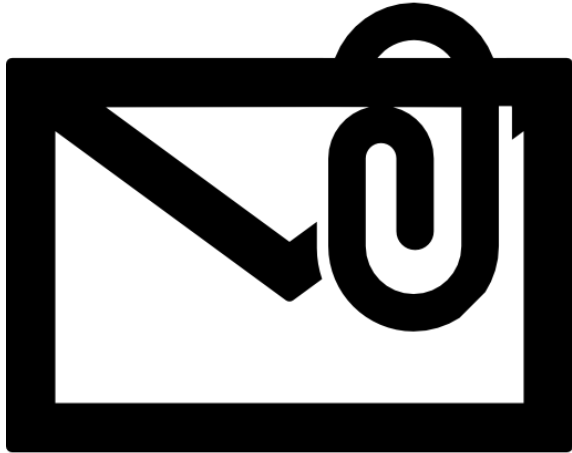


Rester vigilant !

Quand vous recevez un mail, vérifier l'expéditeur et son adresse

Quand vous chattez avec une personne sur la toile, elle n'est pas forcément votre amis – IL PEUT S'AGIR DE N'IMPORTE QUI – Cette personne est une inconnue

Attention aux pièces jointes de vos emails



Soyez vigilant avant d'ouvrir des pièces jointes à un courriel, elles colportent souvent des codes malveillants

Une des méthodes les plus efficaces pour diffuser des codes malveillants est d'utiliser des fichiers joints aux courriels

Pour se protéger, ne jamais ouvrir les pièces jointes dont les extensions sont les suivantes : **.pif** (comme une pièce jointe appelée photos.pif) ; **.com** ; **.bat** ; **.exe** ; **.vbs** ; **.lnk**