

Quelques règles de sécurité informatique

METTRE UN MOT DE PASSE SUR SON ORDINATEUR :

Tous les ordinateurs doivent avoir un mot de passe. Les meilleurs mots de passe sont composés de minimum 8 caractères comprenant des lettres, des chiffres, des symboles, des signes de ponctuation, des majuscules et des minuscules. Ce genre de mot de passe étant plus difficile à retenir, utilisez une méthode mnémotechnique.

Créez par exemple une phrase facile à retenir pour vous :

« Mon équipe de football est la meilleure » et transformez-la en phrase codée en prenant les premières lettres de chaque mot : medfelm puis incorporez des signes, majuscules... cela peut donner : Me2F,eLm&.

Pensez à changer votre mot de passe régulièrement (tous les trois mois).

Ce qu'il ne faut pas faire :

- utilisez un mot, ou une idée simple (« football » ou « amour », par exemple),
- utilisez un élément de votre vie personnelle (date de naissance, prénom...),
- utilisez une suite logique type 123456...
- Envoyez votre mot de passe par mail, l'écrire sur un papier...
- Donnez votre mot de passe. Seul votre coordinateur doit pouvoir accéder à votre ordinateur en cas d'absence.

CONFIDENTIALITE

Si votre ordinateur contient des informations personnelles, merci de les ranger dans un dossier clairement identifiable nommé « personnel » et séparé des autres dossiers.

METTRE A JOUR SES LOGICIELS DE PROTECTION :

Attraper un virus est rapide, il suffit de copier un fichier infecté sur votre ordinateur. Ce fichier infecté peut provenir de n'importe quelles sources extérieures : fichiers téléchargés sur Internet, pièce-jointe de mail, clé USB, disque dur externe, carte SD (appareil photos)... Une fois le virus activé, son action dépend de son concepteur. Il peut détruire immédiatement tout un disque dur, ou encore s'auto-dupliquer par le système de messagerie et envoyer un message à toutes les adresses de votre carnet avec une copie de lui-même en pièce jointe.

Nos ordinateurs sont protégés par le logiciel anti-virus Kasperski. Mettez-le régulièrement à jour. Effectuez également des analyses régulières de votre ordinateur en utilisant Kasperski. Vérifiez aussi que votre pare-feu est bien actif !

ANALYSER LES ELEMENTS PROVENANT DE L'EXTERIEUR

Dès que vous connectez un élément extérieur à votre ordinateur (clé USB, disque dur externe, carte SD...) ou que vous téléchargez un fichier venant d'internet ou de votre boîte mail **vous devez utiliser Kasperski pour l'analyser !** Même si vous avez confiance en la personne qui vous prête son matériel ou même si ce matériel est le vôtre.

Une clé USB, par exemple, passe souvent de main en main et les propriétaires savent rarement qu'elles sont infectées ! C'est un vecteur important de diffusion des virus.

En analysant les fichiers ou les appareils connectés à votre ordinateur, vous réduisez de beaucoup les risques.

SAUVEGARDER SES DONNEES

Sauvegardez régulièrement les documents importants de votre ordinateur, au minimum une fois par semaine **tous les vendredis avant de quitter le bureau.**

Il existe un disque dur externe mis à votre disposition pour effectuer cette opération qui ne prend que quelques minutes.