Utilité et nécessité de disposer d'une bonne politique de mot de passe.

Chaque utilisateur de PC est identifié dans son CPAS par deux éléments :

1. son UID (user identification), c'est-à-dire son nom d'utilisateur ;
2. son mot de passe.

Le UID (exemple : jdupont ou jvandersteen) est défini par le gestionnaire système du service informatique afin de pouvoir gérer plus facilement les accès des différents utilisateurs.

A. Quelques règles s'appliquent aux mots de passe afin de les sécuriser :

- ✓ le mot de passe est **strictement personnel** : ne le confiez à personne ;
- ✓ un mot de passe est **unique,** n'utilisez pas votre code deux fois. Ne réutilisez pas vos mots de passe, renouvelez-les.
- ✓ un mot de passe doit être **changé régulièrement,** soit tous les trois mois au plus tard ;
- ✓ l'idéal est de disposer d'un mot de passe **difficile à trouver mais facile à retenir** (voir systèmes conseillés en fin de note)**;**
- ✓ n'inscrivez votre mot de passe nulle part, ni sur votre sous-main, ni sur un petit papier collé au PC, ni dans un fichier électronique ;
- ✓ lorsque vous allez sur internet , ne cochez pas l'option permettant d'enregistrer votre nom et votre mot de passe (en Internet Explorer, aller dans Tools, Options, Content, Auto complete, décocher User names… et Complete passwords);

- ✓ n’utilisez pas un programme offert et vous permettant de vous rappeler vos mots de passe à tout moment car ces programmes sont souvent des utilitaires pouvant eux-mêmes être utilisés par l’extérieur pour trouver vos mots de passe ;
- ✓ lorsque vous quittez, même temporairement, votre place de travail et votre PC, activez votre écran de veille (screensaver) désactivable uniquement en introduisant votre mot de base ;
- ✓ ne tapez pas votre mot de passe devant une personne susceptible de le lire (par dessus votre épaule par exemple) ;
- ✓ n’essayez ni de voir ni de connaître le mot de passe composé par quelqu’un d’autre ;
- ✓ il est interdit par quelque moyen que ce soit de tenter de connaître ou de voler le mot de passe d’une autre personne ;
- ✓ lorsqu’un mot de passe est utilisé fautivement trois fois de suite (5 fois au maximum), l’accès au système ou au programme doit être bloqué automatiquement et seul le gestionnaire système ou le conseiller en sécurité pourra rétablir l’accès.

Le système de single sign on (signature unique) permet de n’introduire qu’un seul mot de passe par utilisateur lui donnant automatiquement accès à toutes ses applications (quel que soit le langage informatique installé).

NB : il n’est pas autorisé d’installer un programme extérieur tel que Messenger qui donne la possibilité à d’autres personnes mal intentionnées de décoder le mot de passe et de rentrer dans votre PC à distance;

Ne laissez donc ni programme ni toute autre personne à l’exception du gestionnaire système gérer vos accès en interne et en externe. En cas de doute sur la présence d’un tel programme, n’hésitez pas à faire appel au service informatique.

B. Changer régulièrement de mot de passe est important car :

- un pirate discret pourrait se contenter d'observer vos informations sans laisser de traces. En changeant le mot de passe, il ne pourra plus se représenter sur votre compte (votre accès réservé) s'il a été pénétré.

Voici quelques mots de passe à éviter :

- votre **numéro de téléphone ;**
- votre nom ou prénom ;
- votre numéro de plaque minéralogique ;
- votre numéro de sécurité sociale ;
- votre **surnom**, même intime ;
- votre **taille, pointure, poids ;**
- le nom de votre petit(e) ami(e) ou de votre femme ou mari ;
- le nom de votre animal domestique : chien, poisson, …ou toute autre combinaison de ces mots même dans le désordre.

C. Un bon mot de passe ne figure pas non plus dans :

- un **dictionnaire** (surtout électronique, tels que les dictionnaires orthographiques ou techniques) ;
- une **revue ;**
- un **recueil** de bons mots ;
- un recueil de prénoms ;
- un **fichier ou listing informatique .**

D. Quel mot de passe choisir ?

Par définition, un mot de passe doit avoir :

- au moins 8 symboles,
- des chiffres, des lettres et des caractères tels que :,+-, etc.

Attention : évitez quand même les lettres avec accent telles que : é, è, ë, ê, etc.

Quelques astuces.

Le titre d'un livre ou d'un film.

Exemple : **A**lice **a**u **p**ays **d**es **m**erveilles – **s**neewwitje **e**n **d**e **z**even **d**wergen. En prenant la première lettre de chaque mot de ce titre peut être extrait le mot de passe suivant : aapdm - sedzd. Comme ce mot de passe est toutefois trop facile à casser par un pirate et qu'il devra être changé tous les 3 mois, on lui rajoute un chiffre ou une séquence. Exemple : aapdm0803 (mois et année) – sedzd0803, aapdm3803 (numéro de la semaine et année)- sedzd3803. Pour répondre aux normes de sécurité, on rajoute $ ou $, exemple : aapdm3803$

On peut naturellement compliquer le mot de passe à volonté en prenant la deuxième lettre de chaque mot ou les deux premières lettres de chaque mot.

Le cryptage maison.

On peut appliquer une autre technique très simple. En choisissant le titre d'un film ou d'un livre, on prend la première lettre de chaque mot et on intercale le nombre de lettres de chaque mot. Exemple : **A**ls **e**en **j**onge **h**ond d'Hugo Claus ou **V**oyage **a**utour **d**e **m**a **c**hambre de Xavier de Maistre donneront les mots de passe suivants: a3e3j5h4 – v6a6d2m2c7. Une autre possibilité est aejh3354 ou vadmc66227. N'oubliez pas de rajouter un symbole tel que +, $, $, =.

Evitez toutefois de former un mot ayant une signification car les logiciels utilisés par les pirates utilisent des dictionnaires.

L'association.

L'association des mots peut également être utilisée pour élaborer un mot de passe mais il faudra veiller à le compliquer.

Exemple : lavitaebella devra être complété avec des signes : la+vita-e/bella*, mot de passe auquel des chiffres devront être rajoutés.

A noter que la fiabilité de ce mot de passe n'est pas la meilleure.

La simplification.

Cette technique consiste à supprimer toutes les lettres en double dans un mot. Exemple : ''vergelijken'' devient ''verglijkn'' auquel on rajoutera des chiffres et des symboles. Autre exemple : ''serveur'' deviendra ''servu'' auquel on peut rajouter les chiffres suivants : nombre de lettres du mot serveur et nombre de lettres du mot de passe ainsi que l'année et le symbole: servu7503*.

Conclusion.

A vous de trouver la combinaison qui vous semble la plus facile à retenir mais n'oubliez jamais qu'aucun mot de passe n'est inviolable. Si vous appliquez ces conseils, il sera cependant nécessaire au pirate de passer beaucoup plus de temps pour le craquer.