Un peu de sécurité numérique

Quelques règles de base

Sauvegarder ses données régulièrement

9 entreprises sur 10 qui perdent leurs données informatiques font faillite. Quand on est enseignant, perdre ce qu'on a mis du temps à construire est toujours un traumatisme.
C'est pourquoi il est indispensable de réaliser des sauvegardes fréquentes de votre travail. Dans ce cadre, une simple clé USB ne suffit pas : elle peut du jour au lendemain devenir inutilisable, vous pouvez la perdre, la retrouver au fond de la machine à laver... Il est donc conseillé de disposer d'un matériel fiable (disque dur externe par exemple) que vous déposez dans un lieu sûr, que vous ne promenez pas.
A ce titre, l'Owncloud académique peut rendre bien des services (voir sur le site de Dijon Est).

Faire ses mises à jour régulièrement

Quel que soit le système d'exploitation et les logiciels utilisés, ils comportent des failles de sécurité. C'est pour cette raison qu'il est indispensable de faire les mises à jour système et logicielles proposées.

Contrôler les permissions des comptes utilisateurs

Les utilisateurs de Mac Os et de Linux sont beaucoup moins sujets que les utilisateurs de Windows aux virus pour de multiples raisons et notamment parce que, lorsqu'ils utilisent leur ordinateur, ils ne sont identifiés que comme utilisateur avec des droits restreints.
Sous Windows, on devrait travailler également avec un compte "utilisateur" et pas avec un compte "administrateur". C'est contraignant mais plus sûr.

Être vigilant sur les liens ou les pièces jointes contenus dans des messages électroniques

C'est sans doute là l'enjeu le plus important.

Soyez attentifs aux deux points suivants :

- un pirate peut chercher à obtenir des identifiants et mots de passe en vous renvoyant vers un site qui imite celui que vous utilisez habituellement. Par exemple, il crée une fausse page d'accueil du webmail académique et récupère les

données des internautes qui se connectent. Lorsqu'on vous envoie un message qui contient un lien, vérifiez toujours l'adresse de ce lien. Pour ce faire, cliquez droit sur le lien, choisissez "copier l'adresse du lien" puis collez-la dans un traitement de texte par exemple. L'adresse vers laquelle le lien renvoie peut être très différente de celle affichée dans le message... Si vous avez déjà cliqué, pas de panique : regardez attentivement l'adresse dans la barre du navigateur. Globalement, si vous souhaitez aller sur le webmail, utilisez votre raccourci habituel et pas un lien de message. C'est vrai également pour un usage personnel (sites des banques, PayPal,...).

Petit exemple amical ci-après : cliquez (CTRL + clic) https://webmail.ac-dijon.fr
Vous avez donné votre mot de passe ? Changez-le au plus vite à partir du webmail (voir plus bas).

- Un pirate peut vous envoyer un courriel avec une pièce jointe infestée par un virus. Ce virus va lui permettre, par exemple, de récupérer tout ce que vous saisissez au clavier et donc les identifiants et mots de passe...
  Les messages sont parfois très bien faits : vous pouvez avoir l'impression que le contenu est cohérent, vous connaissez l'expéditeur.
  En cas de doute (fautes d'orthographe étranges, message trop respectueux avec des majuscules partout (!), message écrit en lettres capitales, texte écrit trop gros...) :
  * faites "répondre" : vous pouvez afficher l'adresse de réponse (qui est parfois très éloignée de l'adresse de la personne censée avoir envoyé le message) ;
  * demandez confirmation à la personne qui est censée vous avoir envoyé le message.
  Vous avez cliqué trop vite ? Une analyse antivirus s'impose. Il peut aussi être important de déconnecter l'ordinateur d'internet tant que les vérifications ne sont pas faites.

Utiliser des mots de passe solides

12 caractères avec des lettres minuscules, majuscules, des chiffres, des signes de ponctuation et qu'on change de temps en temps...

Marie Petit, habitant Dijon, née le 12/03/1970 pourra créer un mot de passe du type :

MpAeRt21000;1203

ANNEXE

Changer son mot de passe dans le webmail.

Se connecter au webmail, aller dans "Options", "Modifier le mot de passe", se ré-identifier puis changer son mot de passe.