5 pratiques sécuritaires à adopter

Vous avez sûrement entendu parler d'une CS de la région Chaudière-Appalaches qui a été victime de pirates informatiques il y a quelques mois. Ces derniers demandaient une importante rançon en retour de l'ensemble des données informatiques de la CS qu'ils avaient réussi à crypter suite à une attaque informatique. Les responsables de la CS ont immédiatement alerté les forces de l'ordre et ils n'ont évidemment pas payé la rançon, mais les employés et élèves ont perdu l'accès à toutes leurs données ainsi qu'à tous les ordinateurs, photocopieurs et imprimantes pendant plus d'un mois. Même après 4 mois de travail intense de la part des services techniques, plusieurs données n'ont pas été récupérées. Malheureusement, ce n'est pas un cas unique. Le marché mondial de ces « ransomware » est évalué à 1 million de dollars par jour. Bref, une réelle histoire d'horreur que l'on ne veut vraiment pas vivre au travail ou à la maison.

Voici 5 pratiques sécuritaires qui vous aideront à éviter de tomber dans les pièges que tendent ces pirates :

1. Ne pas ouvrir les **fichiers joints à des courriels** qui portent l'extension **.ZIP** ou **.exe**
   Dans les très rares exceptions où ce type de fichier serait partagé par courriel pour une bonne cause, validez auprès de la personne avant d'ouvrir le fichier.

2. Refuser les **offres** sur des sites Web qui vous proposent d'installer quoi que ce soit
   N'installez rien qui est le résultat d'une offre à moins d'être certain de bien pouvoir juger de la provenance. Si vous êtes à la recherche d'un fichier d'installation, sachez faire la différence entre les sites légitimes et les nombreux sites frauduleux qui offrent des logiciels malveillants.

3. Choisir des **mots de passe** sécuritaires et différents pour vos accès
   Au minimum 7 caractères
   Aucune référence à quelque chose qui a du sens
   Utilisation de différents types de caractères
   Implication de la majuscule

4. Refuser de divulguer **des informations personnelles** suite à des demandes électroniques
   Les compagnies ne vous demanderont jamais d'aller sur leur site en vous offrant un hyperlien et à y inscrire vos données. Si vous avez des demandes en ce sens, vous êtes probablement en présence d'une tentative d'hameçonnage.

5. Garder son **mot de passe** pour soi
   Plutôt que d'offrir votre mot de passe à un suppléant ou à un remplaçant, vous devriez partager les fichiers en question en utilisant, par exemple, un répertoire partagé dans OneDrive. Si vous avez absolument à partager un mot de passe, assurez-vous que ce dernier n'est utilisé que pour le service à partager et qu'il est différent de tous vos autres accès. Étant donné que votre mot de passe du réseau CSVDC est inévitablement le même pour votre courriel, votre session Windows, GIF, WordPress, le CSI et le centre d'identité, vous ne devriez pas le partager.

Je vous invite à partager ces pratiques sécuritaires avec vos élèves dans le cadre de vos prochaines utilisations technologiques en classe et n'hésitez pas si vous avez des questions ou des suggestions pour jeudi prochain!