Université de Saint-Boniface

NUMÉRO 45 / OCTOBRE 2020

Notes pratiques

sur la sécurité de l'information

OneDrive et la sécurité

Au mois d'aout 2020, l'USB a lancé la plateforme Microsoft 365. Ce service offre une gamme de logiciels tels que OneDrive.

OneDrive est une application qui vous permet d'accéder à un service d'hébergement et de synchronisation de fichiers de Microsoft. C'est un service semblable à Google Drive et Dropbox. Avec OneDrive, vous pouvez accéder à vos fichiers et les modifier depuis tous vos appareils. Vos fichiers sont protégés dans le nuage. Le partage de dossiers se fait plus facilement, et l'organisation et la récupération de fichiers, plus rapidement. L'espace fourni par le compte Microsoft 365 de l'USB est de 1 To. En effet, votre compte OneDrive peut agir comme votre espace personnel (lecteur F).

Le OneDrive est comme un disque dur dans le nuage qui permet également la collaboration et le partage de fichiers en temps réel.

De nos jours, nous avons tous d'énormes quantités de documents textuels, photos, vidéos et autres données que nous voulons protéger. Stocker les données localement (lecteur C) peut être risqué, car un disque dur peut devenir corrompu et un appareil mobile peut être perdu, volé ou brisé. Le nuage est un endroit idéal pour stocker des données et un moyen simple d'augmenter votre espace de stockage.

Est-ce que OneDrive est sécuritaire?

Les données transmises vers le nuage OneDrive de Microsoft 365 sont chiffrées. Il s'agit d'un chiffrement robuste qui garantit la protection de vos données contre les pirates informatiques. Les données sont également hébergées au Canada.

De plus, afin de mieux sécuriser nos données à l'extérieur de l'USB, Microsoft demande une seconde vérification, appelée authentification multifacteur (*multifactor authentication – MFA*). Il s'agit donc d'un processus pour lequel l'utilisateur est invité à fournir une forme d'identification supplémentaire, consistant, par exemple, à entrer un code sur son téléphone portable ou à utiliser l'application Microsoft Authenticator. L'utilisation d'un mot de passe uniquement ne protège pas complètement contre des attaques. Quand on exige une deuxième forme d'authentification, la sécurité est accrue, car ce facteur supplémentaire n'est pas un élément facile à obtenir ou à dupliquer par piratage.

Pour toute question concernant la *Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP)*, la *Loi sur les renseignements médicaux personnels (LRMP)* ou la sécurité de l'information, veuillez communiquer avec Carole Pelchat, au poste 398 ou à cpelchat@ustboniface.ca.