CYBER READINESS
INSTITUTE

Conserver la sécurité des éducateurs et des étudiants

Les éducateurs et les étudiants de notre pays se trouvent en territoire inconnu alors que l'enseignement à distance devient la norme pour les systèmes scolaires de tout le pays. L'enseignement à distance offre des possibilités extraordinaires que nous n'aurions pas pu imaginer il y a 30 ou 40 ans.

Pour les enseignants, cela signifie que leur mission peut se poursuivre. Pour les élèves (et les parents), cela signifie que la salle de classe n'a pas de limites et qu'un sentiment de normalité peut exister en ces temps incertains.

Nous avons la chance que les technologies avancées d'aujourd'hui permettent aux enseignants et aux élèves de continuer à travailler ensemble. Cela signifie également que nous devons prendre des précautions pour nous assurer que nous sommes tous protégés.

Les enseignants peuvent prendre certaines mesures simples pour protéger leur sécurité en ligne et celle de leurs élèves.

L'essentiel

Mots de passe/phrases de passe

Les mots de passe et phrases de passe restent le meilleur moyen de verrouiller les données personnelles et les applications. L'enseignement à distance signifie également que nous devons tous nous concentrer sur la sécurisation de nos réseaux domestiques.

- Assurez-vous que le mot de passe/la phrase de passe de votre routeur domestique (les phrases de passe sont plus sûres que les mots de passe) ne soit pas facile à deviner et n'inclut pas votre adresse ou vos noms personnels.
- Activer l'authentification multiple (mot de passe/phrase de passe + une autre exigence telle qu'un message textuel) pour accéder à des données critiques dans les applications en cloud, ce qui est important pour le partage de données et de documents avec vos étudiants.

Correctifs de sécurité

Les correctifs de sécurité du système d'exploitation doivent être acceptés et rester à jour.

- Assurez-vous que vos systèmes d'exploitation soient réglés afin de permettre une mise à jour automatique.
- Acceptez tous les correctifs de sécurité pertinents sur une base hebdomadaire.

Hameçonnage

- Plus nous serons nombreux à être en ligne dans les semaines à venir, plus nous pouvons nous attendre à une augmentation des escroqueries en ligne, le piratage psychologique et les attaques d'hameçonnage (*phishing* en anglais). Les pirates et les criminels ne manqueront pas d'utiliser les inquiétudes concernant la propagation du virus et le désir insatiable d'obtenir des informations pour tromper les gens.
- Utilisez des objets cohérents dans vos courriels avec vos élèves afin qu'ils puissent plus facilement savoir qu'ils viennent de vous.
- Passez toujours la "souris" sur le nom de l'expéditeur du courriel pour déterminer la véritable origine de l'expéditeur.
- Rappelez à vos élèves de prêter une attention particulière au nom et à l'adresse électronique de l'expéditeur.

Utilisation des clefs USB

Tout le monde travaillant à distance, nous sommes tentés d'utiliser des clefs USB ou des supports amovibles pour transférer des informations - d'un ordinateur scolaire à un ordinateur domestique.

- Demandez à votre école ou à votre canton s'il est abonné à un fournisseur de stockage de données cloud afin que vous puissiez accéder aux documents et les partager avec vos étudiants de manière sécurisée.
- N'utilisez pas de clés USB. Elles sont souvent infectées par des logiciels malveillants qui peuvent endommager votre ordinateur.

Applications vidéo et chat

- Vous n'avez peut-être pas la possibilité de choisir la plateforme vidéo que vous utilisez parce que les écoles s'engagent pour de grands contrats avec les fournisseurs. Dans la mesure du possible, demandez une plateforme/application de communication sécurisée et cryptée.
- Rappelez à vos élèves - et à vous-même - de bloquer la vidéo et l'audio en désactivant ces fonctions lorsqu'elles ne sont pas utilisées. Vous pouvez également bloquer la caméra vidéo en utilisant un morceau de ruban adhésif épais ou une diapositive vidéo.
- Assurez-vous que vous connaissez la personne qui essaie de discuter avec vous par vidéo.

Comment Facilitez la vie de vos étudiants

Apprenez à vos élèves l'"ABC" de la bonne "cyberhygiène" :

R – Authentifiez vos comptes en utilisant des phrases de passe robustes.

B – Méfiez-vous des tentatives d'hameçonnage et aidez les élèves à vérifier que vous êtes le l'expéditeur du courrier électronique.

C – Avertissez les étudiants de n'utiliser leur application vidéo que s'ils VOIENT votre nom sur l'écran d'appel.