Thème de la semaine 1: **Travailler, enseigner et apprendre de n’importe où**

MOIS DE LA CYBER-SENSIBILISATION

Bonnes pratiques de mot de passe

Astuces à retenir pour les mots de passe

- ✓ Utilisez un mot de passe différent pour chaque site Web, compte utilisateur ou appareil
- ✓ Modifier les mots de passe par défaut
- ✓ Évitez les choix évidents, une référence que quelqu'un d'autre pourrait deviner, des détails personnels ou des mots ou expressions courants
- ✓ Utilisez un mot de passe robuste (8 caractères ou plus (c'est mieux), composé de lettres minuscules, de majuscules, de chiffres et de caractères spéciaux) ou une phrase de passe (au moins 4 mots et 15 caractères de long)
- ✓ Vérifiez la fiabilité de votre mot de passe ou phrase de passe à l'aide de l'outil “How Secure is my Password” (outil en anglais)
- ✓ Protégez votre mot de passe et ne le partagez avec personne
- ✓ Vérifiez si le mot de passe que vous utilisez a été compromis à l'aide de l'outil “Have I been Pwned” (outil en anglais)
- ✓ Activez l'authentification multi-facteur dans la mesure du possible
- ✓ Si vous soupçonnez qu'un compte ou un mot de passe a été compromis, modifiez-le immédiatement
- ✓ Envisagez un gestionnaire de mots de passe pour gérer vos mots de passe. Faites vos recherches avant de sélectionnez d'un gestionnaire de mots de passe
- ✓ Connectez-vous uniquement à partir de sources sûres

Ce que vous devez savoir

Il y a une raison pour les astuces ci-dessus. Évitez d’être victime des cyberattaques suivantes:

- Lors d’utilisation de mots de passe faibles – **Force brute** : La forme d'attaque la plus courante, où un pirate tente des combinaisons de mots de passe possibles en commençant par les mots de passe les plus faciles à deviner.
- Lors d'utilisation de mots courants - **Attaque par dictionnaire** : Où un pirate essai des mots communs.
- Lors d'utilisation du même mot de passe sur plusieurs comptes – **Credential Stuffing** : Où un pirate utilise une liste de noms d'utilisateur et de mots de passe volés en combinaison sur différents comptes, en les essayant automatiquement encore et encore jusqu'à ce qu'une correspondance soit trouvée.

Créé en collaboration avec ECNO, les membres participants d'OASBO ICT et le ministère de l'Éducation pour le Mois de la cyber-sensibilisation M-12 2020.