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

Astuces pour protéger vos appareils

Vos appareils mobiles et ordinateurs contiennent une quantité phénoménale d'information sur vous : vous ne voudriez pas que celle-ci tombe entre les mains d'un cybercriminel. **C'est pourquoi nous vous avons préparé une liste d'astuces pour protéger vos appareils et vos données.**

Assurez-vous de respecter les politiques et les procédures de votre conseil scolaire s'il vous fournit un appareil.

Téléphones intelligents et tablettes

SÉCURITÉ

- Choisissez un mot de passe robuste et activez le verrouillage automatique.
- Activez l'authentification multifacteur.
- Désactivez les fonctions Bluetooth lorsque vous ne les utilisez pas.
- N'utilisez jamais de réseau wifi public ou privé non sécurisé pour consulter des données sensibles.
- Ne laissez jamais un appareil dans votre véhicule ou sans surveillance en public.
- N'envoyez pas de données sensibles ou personnelles par message texte.
- Mettez à jour votre système d'exploitation et activez les mises à jour automatiques.

APPLICATIONS

- Désinstallez les applications dont vous ne vous servez plus.
- Vérifiez les permissions de vos applications et méfiez-vous des applications qui demandent l'accès à des données peu pertinentes à leurs fonctions.
- Désactivez la localisation lorsque vous ne l'utilisez pas.
- Désactivez toute fonctionnalité dont vous n'avez pas besoin.
- Ne téléchargez pas d'applications développées par des organisations sur lesquelles peu d'information est disponible.
- Ne téléchargez que des applications de sources fiables, comme l'App Store ou Google Play.

Ordinateurs portables et de bureau

- Installez un logiciel de sécurité comme un antivirus et une protection contre les logiciels espions, et effectuez des analyses de sécurité au moins une fois par semaine.
- Verrouillez votre appareil à l'aide d'un mot de passe robuste ou d'une phrase de passe.
- Activez l'authentification multifacteur partout où vous le pouvez.
- Renforcez votre navigateur :
  - Dans le menu déroulant du navigateur, sélectionnez les paramètres de sécurité les plus stricts.
  - Faites régulièrement les mises à jour de votre navigateur si elles ne sont pas automatiques.
  - Videz votre cache et votre historique de navigation pour effacer les données sensibles comme les identifiants, les mots de passe et les renseignements bancaires de la mémoire du navigateur.
- Mettez vos logiciels et votre système d'exploitation à jour et activez les mises à jour automatiques.
- Soyez prudents lorsque vous téléchargez des fichiers en ligne; assurez-vous que la source est fiable.

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.