Cyber-hygiène

Cyber-sensibilisation pour la rentrée scolaire réussie

Assurez-vous de connaître le code de conduite en ligne de votre école, les politiques d'utilisation appropriée des technologies à partir des appareils et logiciels fournis par l'école, ainsi que les politiques encadrant l'utilisation d'appareils et téléphones personnels (PAP, ou « prenez vos appareils personnels »).

Sécurité de vos appareils personnels

Assurez-vous de télécharger vos applications à partir de magasins d'application officiels afin d'éviter l'installation d'applications potentiellement dangereuses.

Méfiez-vous des extensions de navigateur et des modules complémentaires. Bien qu'ils puissent sembler inoffensifs, certains peuvent recueillir vos données, vous escroquer, afficher des publicités indésirables ou saisir le contrôle de votre navigateur. Ne téléchargez du contenu qu'à partir de sources officielles.

Réglez et mettez à jour les paramètres de confidentialité – Ajustez vos réglages au plus haut degré de confidentialité sur tous vos appareils et dans toutes les applications.
Vérifiez régulièrement ces réglages, car ils pourraient avoir été modifiés à la suite d'une mise à jour.

Réglez et mettez à jour les autorisations des applications – Désactivez celles qui sont devenues inutiles. Faites particulièrement attention aux applications qui ont accès à la localisation de votre appareil, à votre liste de contacts, à votre appareil photo, à votre espace de stockage et à votre microphone. Cette autorisation est-elle nécessaire?

Activez le verrouillage automatique de votre appareil – Définissez un NIP ou un mot de passe unique avec données biométriques pour chacun de vos appareils, et activez le verrouillage automatique lorsque ceux-ci sont en veille.

N'utilisez que des points d'accès Wi-Fi sûrs et évitez d'utiliser les points d'accès Wi-Fi publics sans VPN.

Dans le cyberespace, la prudence est de mise

La rentrée scolaire est un moment excitant pour tout le monde. Malheureusement, c'est aussi le cas pour les cybercriminels. En effet, ceux-ci en profitent pour cibler les enfants peu familiarisés avec les risques en ligne. Considérez les sujets de discussion suivants et encouragez les questions et le dialogue :

- Les cybercriminels : qui sont-ils et que font-ils?
- Que font les cybercriminels avec nos renseignements personnels?
- Comment les enfants peuvent-ils rester en sécurité?

Mots de passe forts et authentification multifacteur

La rentrée scolaire est un moment propice pour revoir les éléments d'un bon mot de passe.
Voici quelques trucs simples qui vous aideront à assurer la sécurité de vos comptes et de vos appareils.
Plus long, plus sûr. Privilégiez des mots de passe d'au moins 15 caractères.

- MAJUSCULES, minuscules, $ymbo!es et chiffr3s : mélangez-les pour créer des mots de passe forts.
- Utilisez une phrase significative comme mot de passe afin de vous en souvenir plus facilement, par exemple, « MonMignonHamsterMaurice » ou « ViveLeCampDeBasketball ».

Sécurité de vos comptes personnels

- **Faites la liste de tous vos comptes d'utilisateur** et supprimez ceux dont vous n'avez plus besoin.
- **Pensez à créer des comptes distincts** pour les amis et la famille, le travail, et les jeux et médias sociaux.
- Si possible, **activez l'authentification multifacteur (AMF)** pour chacun de vos comptes d'utilisateur pour renforcer leur sécurité.
- **Définissez un mot de passe fort ou une phrase solide** à l'aide des trucs ci-dessus.
- **Activez les notifications d'activités suspectes** pour chacun de vos comptes d'utilisateur.
- **Ne vous connectez pas** automatiquement aux applications avec vos identifiants de compte de médias sociaux.
- **Ne reprenez pas** L'identifiant et le mot.

Financé par :

Ontario

/{MOI} NUMÉRIQUE

Pour plus d'informations : www.ecno.org/cyber-sensibilisation