Septembre

Cyberhygiène

Sensibilisation à la cybersécurité pour la rentrée scolaire

Cyberhygiène: pour assurer la sûreté des appareils

Les ordinateurs, téléphones et tablettes stockent tous des renseignements personnels convoités par les cybercriminels. Il est important de sécuriser adéquatement ses appareils en respectant les règles de base de la cyberhygiène pour éviter que ses informations tombent en de mauvaises mains.

Voici quelques conseils :

- Installer un **antivirus** et un **anti-logiciel espion**, la première ligne de défense con¬tre les cybercriminels.
- Activer la mise à jour automatique – les mises à jour peuvent être programmées pour être téléchargées et l'installées la nuit.
- Consulter régulièrement les **paramètres de confidentialité** et limiter les informations que les autres peuvent voir.
- Verrouiller les appareils à l'aide de **l'empreinte digitale**, la reconnaissance faciale, d'un **code** ou d'un **mot de passe**.
- Garder les **paramètres de navigateurs** à jour et effacer régulièrement les **données de navigation**.

Soyez cybervigilante et cybervigilant

Pour beaucoup, la rentrée scolaire est un moment excitant. Malheureusement, les cybercriminels en profitent d'exploiter les jeunes peu familiers avec les risques en ligne. Pensez à aborder les sujets suivants avec les enfants:

1. Les cybercriminels, qui sont-ils et que veulent-ils?
2. Que font-ils avec nos informations?
3. Comment se protéger?

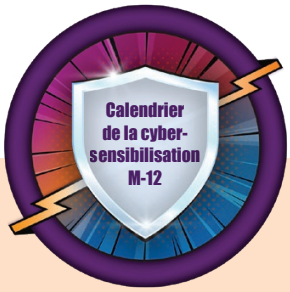
Se protéger en utilisant des mots de passe ro¬bustes et l'authentification multifactorielle

La rentrée scolaire est une bonne occasion de se rap¬peler ce qui fait la sûreté **d'un bon mot de passe.** Voici quelques conseils:

1. Choisir un **mot de passe long**, préférablement de 15 caractères ou plus.
2. Combiner **MAJUSCULES, minuscules, $ymbo!es et n0mbr3s pour renforcer un mot de passe**.
3. Utiliser une phrase secrète pour créer un mot de passe significatif et facile à retenir. Une phrase secrète est une suite de mots comme «MonAdor¬ableHamsterGustave» ou «BasketballÉquipeDeFeu».

En plus du mot de passe, on peut utiliser l'authentifica¬tion multifactorielle (AMF) pour améliorer la sécurité de ses comptes. L'AMF repose sur une combinaison de fac¬teurs pour authentifier une utilisatrice ou un utilisateur.
Exemples de facteurs :

- **Une chose qu'on sait** – comme un mot de passe ou une phrase secrète.
- **Une chose qu'on a** – tel qu'un téléphone ou un jeton.
- **Une chose propre à soi** – tel qu'une empreinte digitale.



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

Ontario