

Prépare-toi à une année scolaire cybersécuritaire!

Tu as beaucoup de choses à découvrir en ce début d'année scolaire : où trouver les meilleures collations sur le campus, comment te réveiller pour le cours de 8 heures et, surtout, comment protéger tes comptes et tes appareils contre le piratage. Voici quelques conseils simples pour t'aider à être en cybersécurité :



Crée des phrases de passe robustes et uniques pour chacun de tes comptes

Même tes comptes apparemment sans importance, comme la plateforme de présentation que tu n'as utilisée que pour un seul cours, doivent être protégés. Les phrases de passe robustes sont composées de quatre mots aléatoires ou plus et comportent au moins 15 caractères – comme ValiseMelonChateauMaison.

Utilise un gestionnaire de mots de passe

Tu as assez de mémorisation à faire ces jours-ci. Laisse les gestionnaires de mots de passe travailler pour toi. Il existe une multitude d'options gratuites ou peu coûteuses, adaptées au budget des étudiants, qui peuvent t'aider à te souvenir de tous tes mots de passe et phrases de passe uniques.

Active l'authentification multifactorielle

L'authentification multifactorielle utilise un processus d'authentification personnelle qui peut inclure ce que tu es (comme l'empreinte du pouce ou la reconnaissance faciale), ce que tu possèdes (comme ton téléphone) et ce que tu sais (comme un code NIP). Active-la sur tous tes comptes et appareils, quand c'est possible, pour les garder en toute sécurité.

Active les mises à jour automatiques

En activant les mises à jour automatiques sur tes appareils et tes applications, tu passeras moins de temps à mettre à jour manuellement tes gadgets et plus de temps à informer tes amis des événements amusants du campus. De plus, tu pourras accéder à de nouvelles fonctionnalités, prévenir les cybermenaces et corriger les bogues. Tu peux même établir un calendrier de mise à jour à des heures précises afin de ne pas interrompre tes périodes d'étude.

Installe un logiciel antivirus

Les logiciels malveillants sont des logiciels malveillants qui infectent tes appareils. L'une des façons les plus courantes d'être infecté par un logiciel malveillant est de cliquer sur des liens et de télécharger quelque chose en ligne. Un logiciel antivirus peut t'aider à protéger tes appareils si tu cliques sur un lien malveillant par accident (*hmm* comme quand toi et tes colocataires essayez de regarder la dernière saison du Bachelor en diffusion en continu!)

Repère les signes d'hameçonnage

Les cybercriminels utilisent l'hameçonnage pour te voler des informations ou de l'argent en se faisant passer pour quelqu'un qu'ils ne sont pas (comme ta banque ou le gouvernement). Ils peuvent aussi se faire passer pour quelqu'un que tu connais, comme ton professeur ou ta camarade de classe. Garde l'œil ouvert sur les messages ou les demandes suspectes. Par exemple, ton professeur ne te demanderait probablement pas des cartes-cadeaux pour débloquer tes notes.

Obtiens d'autres conseils pour vous protéger, toi et tes appareils, pendant cette année scolaire en visitant :

[PensezCybersécurité.ca](https://www.pensezcybersécurité.ca)



Centre de la sécurité
des télécommunications

Communications
Security Establishment

Canada