FORTRA

Terranova Security®

7 conseils de cybersécurité pour les étudiants

Les étudiants utilisent divers appareils et logiciels pour leurs études. Bien qu'ils possèdent également différents niveaux d'expertise technologique, tous les étudiants ont intérêt à suivre ces bonnes pratiques élémentaires en matière de cybersécurité. Cela leur permettra de protéger leurs informations sensibles des cybercriminels et de s'assurer une expérience d'apprentissage agréable et sans risque.

1

CRÉEZ DES MOTS DE PASSE FORTS ET UNIQUES

Chacun de vos comptes en ligne ou appareils doit être protégé par un mot de passe fort et unique, composé d'au moins 12 caractères. Assurez-vous que vos mots de passe soient constitués d'une combinaison de majuscules, de minuscules, de nombres et d'autres symboles. Évitez d'inscrire vos mots de passe sur un bout de papier. Utilisez plutôt un programme de gestion des mots de passe qui permet de stocker et d'organiser vos données en un seul endroit.

2

ACTIVEZ L'AUTHENTIFICATION À DEUX FACTEURS

L'ajout d'une étape d'authentification supplémentai e à vos comptes en ligne ou vos appareils peut renforcer significati ement la protection de vos données. Puisqu'elle demande à l'utilisateur de saisir un mot de passe ou un code additionnel, elle contribue à confirmer otre identité lors de l'ouverture de session. Il devient ainsi plus difficile pour l cybercriminels d'avoir accès à votre information.

3

INSPECTEZ ATTENTIVEMENT TOUS LES NOUVEAUX MESSAGES

Qu'il s'agisse d'un courriel, d'un message texte ou d'un message vocale automatisé, demeurez vigilant et attentif aux signes précurseurs d'une éventuelle cyberattaque. Méfiez- ous des messages non sollicités ou inattendus, même s'ils semblent provenir de contacts connus. Évitez de cliquer sur des liens suspects, de télécharger des pièces jointes douteuses et de transférer de l'argent.

4

SOYEZ EXTRÊMEMENT PRUDENT LORSQUE VOUS PARTAGEZ DES DONNÉES PERSONNELLES

Méfiez- ous des messages qui vous demandent de divulguer vos informations personnelles, même si le ton est urgent et qu'on vous encourage à agir immédiatement. Partagez des informations personnelles en ligne uniquement lorsque vous êtes certain de l'identité du demandeur et que vous savez comment vos données seront utilisées.

5

EFFECTUEZ LES MISES À JOUR DE VOS PROGRAMMES ET SYSTÈMES D'EXPLOITATION

Assurez-vous que tous vos logiciels, systèmes d'exploitation et applications sont à jour en tout temps. Ces mises à jour comprennent souvent des correctifs de sécurité importants qui contribuent à la protection de vos données. Si vous téléchargez une application pour la première fois, vérifiez qu'il s agit bien de la version la plus récente. L'installation et l'utilisation de versions plus anciennes peuvent augmenter votre vulnérabilité face à une cyberattaque.

6

AJUSTEZ LES PARAMÈTRES DE SÉCURITÉ DE VOTRE NAVIGATEUR

La plupart des navigateurs possèdent des filt es intégrés qui protègent vos données des sites Web non sécurisés, des fenêtres pop-up et d'autres menaces. Malgré cela, il est essentiel d'ajuster les paramètres nécessaires pour améliorer votre niveau de sécurité et de confidentialité De plus, supprimez les cookies, videz le cache et effacez l'historique après chaque session Internet pour vous assurer de ne laisser aucune trace de vos données dans le navigateur pour de longues périodes.

7

SIGNALEZ LES ACTIVITÉS SUSPECTES OU MALVEILLANTES

Si vous faites face à un message inattendu ou à un cyberincident, comme la participation d'une personne non autorisée à une visioconférence, signalez-le immédiatement selon la politique en vigueur dans votre établissement. Dans votre logiciel de messagerie, identifiez les messages suspects comme étant des courriels indésirables ou des tentatives d'hameçonnage.