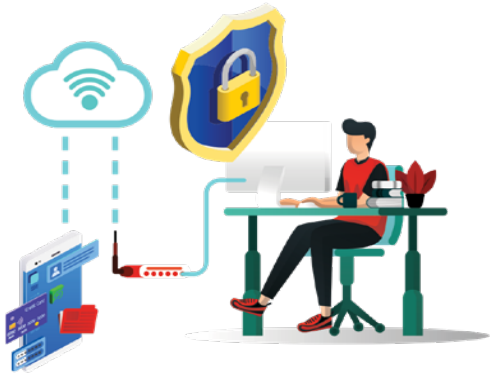
Thème de la semaine 1: Travailler, enseigner et apprendre de n'importe où

Votre réseau est-il bien protégé à la maison?

Évaluez votre réseau à la maison

- ☐ Votre ordinateur fait-il automatiquement ses mises à jour logicielles?
- ☐ Avez-vous activé votre pare-feu personnel?
- ☐ Avez-vous installé un antivirus ou une protection contre les logiciels malveillants sur votre appareil?
- ☐ Avez-vous changé tous les mots de passe et identifiants par défaut de votre routeur?
- ☐ Avez-vous remplacé le nom par défaut de votre réseau sans fil par quelque chose d'unique qui ne trahit ni votre identité ni votre emplacement?
- ☐ Le mot de passe de votre routeur wifi est-il suffisamment robuste?
- ☐ Votre réseau wifi est-il muni de la configuration de sécurité WPA2 (ou mieux, WPA3)?
- ☐ Votre routeur est-il dans un emplacement central de votre maison? (S'il est trop près des murs extérieurs ou des fenêtres, le signal risque de se rendre plus loin que nécessaire.)
- ☐ Le micrologiciel de votre routeur est-il à jour?
- ☐ Utilisez-vous un réseau wifi différent pour vos appareils intelligents connectés (télévision, Amazon Echo, caméra, etc.) et vos ordinateurs portables et téléphones?



Ce que vous devez savoir

En ces temps d'adaptation à l'apprentissage, à l'enseignement et au travail à la maison, la cybersécurité est devenue encore plus importante.

Un réseau mal protégé est une porte ouverte pour les cybercriminels, et si votre routeur se trouve compromis, vous pourriez sérieusement en pâtir : vol d'identité ou d'information, publicités et sites malveillants, fraude et bien plus. De plus, si un cybercriminel pénètre dans votre réseau, il pourrait s'en servir pour commettre des infractions, par exemple pour attaquer d'autres réseaux et appareils.

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.