Semaine 1: Travailler, enseigner et apprendre de n'importe où

Le monde de l'éducation a beaucoup changé récemment. Le travail à domicile, l'enseignement et l'apprentissage dans un environnement à distance ou virtuel sont devenus la "nouvelle norme".

Lorsque vous travaillez au bureau ou dans vos écoles, vous bénéficiez de mesures de sécurité qui protègent nos réseaux, systèmes, appareils et informations contre les cybermenaces.

Passer de cet environnement de confiance à des lieux de travail à distance peut augmenter les risques de sécurité.

Vous apprendrez dans cette vidéo comment vous pouvez aider à protéger les renseignements de votre Conseil et de vos élèves tout en travaillant de n'importe où.

La première source de risque que nous allons examiner est vos appareils.

Lorsque vous êtes assigné un appareil appartenant à votre Conseil, vous ne devriez jamais le partager avec quelqu'un d'autre. Vous devez le garder en lieu sûr, et vous devez suivre les directives fournies par votre Conseil concernant l'utilisation acceptable de l'appareil.

Si vous utilisez un appareil personnel, aucune information privée ou confidentielle ne doit être entreposée sur cet appareil.

Vous ne devez pas acheminer de l'information de vos comptes professionnels à votre appareil personnel. Si vous utilisez un appareil privé, tout travail doit être effectué dans le nuage sécurisé et enregistré à cet endroit.

Les exemples comprennent : D2L/Brightspace, Google Apps Éducation, Microsoft O365 et d'autres applications infonuagiques fournies par votre Conseil.

En accédant à ces applications via un navigateur et en ne téléchargeant pas d'informations sur votre appareil personnel, vous protégez les informations.

Si vous utilisez un appareil personnel, assurez-vous que vous avez un antivirus / anti-malware à jour d'installé, et que le système d'exploitation est à jour.

Si l'appareil est partagé, ayez des comptes de connexion séparés pour toutes les personnes qui le partagent, et assurez-vous que lorsque vous avez terminé le travail, vous fermez tous les navigateurs et déconnectez de tous les comptes nuages.

Si votre appareil du Conseil est perdu ou volé, signalez immédiatement la perte à votre Direction ou votre superviseur, ainsi qu'au centre d'aide et de service informatique de votre Conseil.

La deuxième source de risque que nous allons examiner est votre réseau à domicile.

Votre réseau Wi-Fi à domicile est essentiel pour rendre votre espace de travail cyber-sécurisé.

L'une des façons les plus faciles d'augmenter votre cybersécurité à domicile est de changer le mot de passe Wi-Fi par défaut qui vient avec votre routeur et d'utiliser un mot de passe fort qui est difficile à deviner.

Utilisez seulement les réseaux Wi-Fi dont vous êtes certains sont sécurisés, par exemple celui de votre Conseil ou votre réseau Wi-Fi à domicile. Méfiez-vous de l'utilisation de réseaux Wi-Fi externes tels que dans les cafés, restaurants, hôtels, etc. pour des fins professionnelles.

Les cybercriminels peuvent configurer des réseaux fictifs qui enregistreront votre activité, y compris vos noms d'utilisateur et mots de passe. Ces réseaux ressemblent beaucoup aux réseaux Wi-Fi publics les plus courants.

Une bonne pratique est d'utiliser votre téléphone cellulaire comme point d'accès si vous êtes in certains de la validité du réseau.

La dernière source de risque que nous allons examiner sont les courriels d'hameçonnage.

Les courriels d'hameçonnage essaient souvent de créer un sens d'urgence afin de vous faire peur et vous apporter à cliquer sur un lien ou à divulguer de l'information.

Vous devriez toujours vous méfier de tout courriel vous demandant de mettre à jour vos mots de passe et vos identifiants de connexion.

Si vous soupçonnez qu'un courriel envoyé à votre compte du Conseil est une escroquerie , signalez-le immédiatement au Service informatique de votre Conseil.

Si vous avez cliqué sur un lien et/ou fourni vos identifiants, ne soyez pas gêné, il est essentiel que vous signaliez ces informations immédiatement afin de protéger votre compte et éviter une perturbation plus généralisée.

Si vous recevez un courriel que vous pensez est une escroquerie à votre compte personnel, utilisez les mêmes techniques critiques afin d'analyser si elle pourrait être une escroquerie.

En cas de doute, ne cliquez sur aucun lien et communiquez directement avec l'institution par des moyens sécurisés.

Si vous cliquez sur un lien et entrez vos coordonnées, changez immédiatement votre mot de passe sur ce compte et tout autre compte sur lequel vous avez utilisé le même mot de passe.

Merci d'avoir regardé cette vidéo