Assurer la cybersécurité sur les médias sociaux

Nous voyons souvent des attaques de cybersécurité dans les nouvelles, mais en réalité, les cyberattaques se produisent toujours au moment où l'on s'y attend le moins. Et quand elles se produisent, elles arrivent rapidement à n'importe qui ou à n'importe quel organisme. Nous ne pensons pas toujours à la façon dont nos propres comptes de médias sociaux peuvent nous rendre vulnérables aux attaques de fraude psychologique. Cette semaine, l'unité d'éducation et du Centre d'excellence est là pour vous aider à vous renseigner sur les vulnérabilités en matière de cybersécurité sur les médias sociaux et sur les moyens de rester en sécurité!

Qu'est-ce qui vous rend vulnérable sur les médias sociaux?

- **Publier des renseignements révélateurs sur votre vie personnelle et professionnelle** peut aider les auteurs de menaces à recueillir des données pour des attaques de fraude psychologique contre vous ou votre organisme.
- **Garder les profils publics et accessibles à tous –** en permettant à quiconque d'avoir accès à votre profil, les auteurs de menaces peuvent plus facilement recueillir des renseignements personnels ou sur l'entreprise à partir de votre profil.
- **Accepter tout le contenu sans le vérifier –** et ne pas vérifier si les liens sont sûrs et fiables peut entraîner des attaques de logiciels malveillants ou de rançongiciels.
- **Utiliser les médias sociaux sur des points d'accès Wi-Fi publics –** les Wi-Fi publics sont des endroits courants où les attaquants peuvent accéder à vos données et renseignements. Les attaquants utilisent les réseaux Wi-Fi publics pour intercepter les données et injecter des logiciels malveillants dans les appareils connectés.

Pratiques exemplaires en matière de médias sociaux

- **Gérez vos paramètres de confidentialité et de sécurité –** la gestion de vos paramètres de confidentialité et de sécurité vous aidera à contrôler qui voit et a accès à votre contenu sur les médias sociaux.
- **Faites attention à qui suit votre compte –** n'engagez le dialogue qu'avec les personnes que vous connaissez.
- **Faites attention à ce que vous publiez –** est-ce que je divulgue des renseignements privés sur moi-même ou mon organisme?

- **En cas de doute, ne les publiez pas –** si vous hésitez à publier certains renseignements, gardez-les privés.
- **Cliquez sur les liens avec prudence –** la sécurité des comptes de médias sociaux est régulièrement atteinte. Soyez attentif au langage, au contenu ou au comportement qui sort de la norme.
- **Tenez-vous au courant des politiques de confidentialité –** sachez que les politiques de confidentialité peuvent changer et tenez-vous au courant de leur effet sur vous ou votre organisme.
- **Utilisez les médias sociaux sur un réseau Wi-Fi sécurisé ou des données cellulaires personnelles –** n'utilisez que des points d'accès ou des réseaux de confiance, protégés par un mot de passe.
- **Activez l'authentification multifactorielle (AMF) –** utilisez l'AMF lorsque cela est possible, pour vos comptes de médias sociaux.

Vous voulez en savoir plus?

Les médias sociaux sont un endroit idéal pour que les auteurs de menaces obtiennent des renseignements afin d'élaborer une attaque qui vous ciblera et exploitera spécifiquement vous ou votre organisme. C'est pourquoi il est si important de suivre nos pratiques exemplaires en matière de médias sociaux afin d'assurer votre cybersécurité. Ne manquez pas les semaines à venir pour en savoir plus sur la fraude psychologique et les autres cybermenaces!

Pour plus d'informations, consultez la Bibliothèque des connaissances sur le Portail de l'Ontario pour l'apprentissage pour la cybersécurité.