UTILISATION DE COMPTES PERSONNELS DE MÉDIAS SOCIAUX AU TRAVAIL

MARS 2019

ITSAP.00.066

MÉDIAS SOCIAUX AU TRAVAIL

Les médias sociaux vous permettent d'entrer en contact facilement avec d'autres personnes et de transmettre de l'information instantanément. Comme ces services et plateformes sont maintenant intégrés à nos activités courantes en ligne, de nombreux employeurs permettent à leur effectif d'utiliser les comptes personnels de médias sociaux au travail. Cette utilisation, cependant, peut fournir aux auteurs de menace des points d'entrée faciles et évidents dans les réseaux de votre organisation et ainsi leur permettre d'accéder à votre information. Il se peut également que vous exposiez votre identité en ligne et celle de vos collègues à des risques.

RISQUES LIÉS À L'UTILISATION DE COMPTES PERSONNELS DE MÉDIAS SOCIAUX AU TRAVAIL

Lorsque vous affichez des photos sur Facebook, des gazouillis sur Twitter ou du contenu sur votre page LinkedIn, vos activités peuvent révéler beaucoup d'information à votre sujet ou au sujet de votre organisation qui peut ensuite être exploitée. Les risques comprennent notamment ce qui suit :

MALICIELS ET VIRUS

À l'aide des médias sociaux, les auteurs de cybermenace peuvent transmettre des maliciels (qui peuvent comprendre des virus, des chevaux de Troie et des vers) à des dispositifs et à des réseaux. En cliquant sur un hyperlien abrégé, une photo ou une annonce, vous pouvez ouvrir la porte à de graves cyberattaques visant les dispositifs et les réseaux de votre organisation. Lorsque vous utilisez vos comptes personnels au travail, évitez de cliquer sur tout ce qui vous semble suspect. Avisez l'équipe responsable des TI de votre organisation si vous pensez que votre compte a été compromis.

PIRATAGE PSYCHOLOGIQUE

Plus vous révélez d'information sur les médias sociaux, plus vous êtes susceptibles de devenir la cible d'un auteur de menace. Sachez que dès que vous affichez ou partagez de l'information, celle-ci devient publique et peut ultimement être employée dans le cadre d'arnaques par piratage psychologique bien ficelées. Les auteurs de cybermenace peuvent utiliser cette information pour se faire passer pour vous et envoyer à vos collègues des courriels ciblés contenant des maliciels. Si vos collègues sont dupés et ouvrent le courriel ainsi qu'une pièce jointe, un maliciel peut infecter leur ordinateur et les réseaux organisationnels.

Pour en savoir plus sur le harponnage, consultez la publication ITSAP.00.100, Reconnaître les courriels malveillants, du CCC.

PERTE DE DONNÉES NON INTENTIONNELLE

Il est important de penser aux répercussions avant d'afficher du matériel lié au travail sur un compte personnel de média social. En partageant le lieu physique de l'immeuble où vous travaillez ou en affichant une publication aux allures anodines au sujet d'un projet que vous venez de terminer, sans le savoir, vous aidez peut-être des auteurs de menace à recueillir de l'information sur votre organisation. Même avec les paramètres de confidentialité et de sécurité les plus élevés, un auteur de menace peut compromettre l'un de vos comptes personnels de médias sociaux, il pourrait non seulement obtenir l'accès à vos données personnelles, mais également amasser des données sur les collègues faisant partie de vos contacts. Grâce à ces renseignements, ils peuvent entre autres dresser un portrait plus détaillé de votre structure organisationnelle.

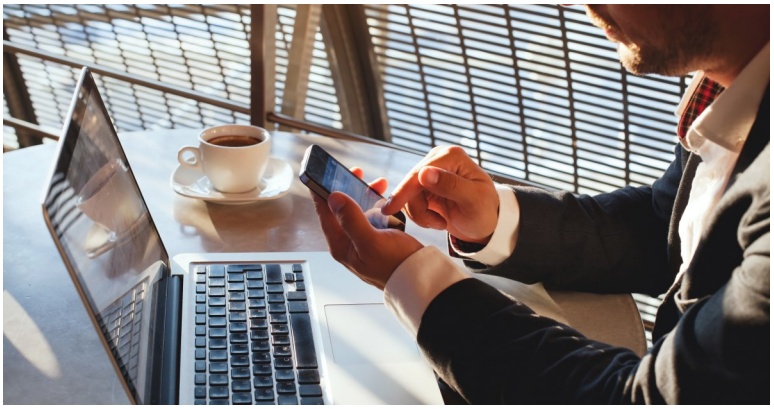
SÉRIE SENSIBILISATION

MESURES D'ATTÉNUATION DES RISQUES LIÉS À L'UTILISATION DE COMPTES PERSONNELS DE MÉDIAS SOCIAUX AU TRAVAIL

- Utilisez un mot de passe ou une phrase de passe (si supporté par le site Web ou l'application) unique et long pour chacun de vos comptes.
- Obtenez l'approbation de vos supérieurs avant d'afficher de l'information liée au travail sur un compte personnel de média social.
- Limitez l'utilisation de services de géolocalisation ou de services géodépendants dans les applications de médias sociaux.
- Utilisez l'authentification à deux facteurs lorsqu'elle est offerte.
- Faites preuve de prudence et éviter d'accepter des demandes d'amitié, d'abonnement ou de contact d'inconnus.
- Méfiez-vous des messages comportant du langage ou du contenu inhabituel.
- Faites preuve de prudence lorsque vous cliquez sur des hyperliens abrégés : ils pourraient vous diriger vers un site malveillant.
- Évitez de révéler des renseignements personnels sur vos comptes de médias sociaux (p. ex. adresse domiciliaire, date de naissance ou NAS). Plus vous partagez d'information, plus vous risquez d'être victime de vol d'identité.
- Passez en revue périodiquement vos paramètres de sécurité afin de contrôler le contenu auquel a accès chaque groupe de personnes.
- Fermez votre session lorsque vous avez terminé d'utiliser vos comptes.

Même si vous prenez toutes ces précautions, avisez immédiatement l'équipe responsable des TI de votre organisation si vous remarquez des anomalies ou si vous pensez que votre compte a été compromis.

Par ailleurs, il est important de noter que lorsque vous indiquez l'endroit où vous travaillez dans votre profil et partagez vos opinions sur les médias sociaux, votre réputation et celle de votre organisation peuvent être ternies. Tout commentaire négatif ou comportement en ligne inacceptable de votre part peut attirer une attention non désirée sur vous et votre lieu de travail.



CONSIDÉRATIONS RELATIVES À L'UTILISATION DE COMPTES ORGANISATIONNELS DE MÉDIAS SOCIAUX

Si vous gérez ou tenez à jour un compte organisationnel de média social, envisagez de mettre en œuvre les mesures ci-dessous afin de réduire la possibilité de compromission du compte.

- Veiller à ce que le personnel ayant les droits de publication ait lu et compris les politiques de l'organisation relatives à l'utilisation d'Internet et des médias sociaux.
- Limiter le nombre de personnes ayant les droits d'administrateur ou de publication pour le compte organisationnel.
- Obtenir une approbation finale avant de publier du contenu sur les comptes officiels ou au moyen de ceux-ci.
- Publier du contenu au moyen d'applications et de dispositifs fiables uniquement.
- Protéger les dispositifs mobiles organisationnels à l'aide d'un mot de passe.
- Installer la plus récente version des navigateurs Web, des systèmes d'exploitation et des applications.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (CCC) à **cyber.gc.ca.**