Centre de la sécurité des télécommunications
Communications Security Establishment

NON-CLASSIFIÉ

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

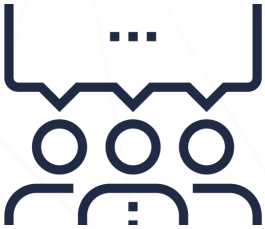
Utilisation de comptes personnels de médias sociaux au travail

Février 2023

ITSAP.00.066

Les 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 et les systèmes de votre organisation. Il se peut également que vous exposiez votre identité en ligne et celle de vos collègues à des risques.



Points à considérer avant de vous joindre à des applications de médias sociaux

- Faites une recherche sur la plateforme de média social que vous souhaitez utiliser et passez en revue l'information à son sujet qui est accessible publiquement.
- Prenez le temps de bien comprendre les politiques de la plateforme concernant la confidentialité, la collecte et l'utilisation des données, les exigences pour les autorisations et les conditions générales d'utilisation afin de savoir quelles données seront consultées et à quels endroits les données seront stockées ou transférées.
- Il est important de bien saisir les détails relatifs à la propriété, au contrôle ou à l'influence, ainsi qu'à la résidence des données – les fournisseurs et les propriétaires de la plateforme sont soumis aux lois de leur région, ce qui pourrait avoir une incidence sur la sécurité et la confidentialité des données des utilisateurs.
- Assurez-vous de connaître les fonctions et les éléments de vos appareils auxquels l'application peut accéder, comme votre caméra, votre microphone, votre emplacement et vos contacts.

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.

- Veillez à ce que les membres du personnel, surtout ceux qui ont les droits de publication, lisent, comprennent et respectent les politiques de votre organisation relatives à l'utilisation d'Internet et des médias sociaux.
- Limitez le nombre d'utilisateurs dans votre organisation qui détiennent les droits d'administrateur ou de publication pour les comptes organisationnels de médias sociaux.
- Assurez-vous que tous les utilisateurs autorisés ont des comptes distincts, avec des justificatifs d'identité uniques, lorsqu'ils publient du contenu.
- Obtenez une approbation finale avant de publier du contenu sur les comptes officiels ou au moyen de ceux-ci.
- Publiez du contenu au moyen d'applications et d'appareils fiables et approuvés uniquement.
- Sécurisez les appareils organisationnels au moyen de l'authentification multifacteur (AMF) et de mots de passe ou phrases de passe forts .
- Installez les correctifs nécessaires et la plus récente version des navigateurs Web, des systèmes d'exploitation, des appareils et des applications .

Série sensibilization

No de cat. D97-1/00-066-2023F-PDF
ISBN 978-0-660-47411-3

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 :

Perte de données non intentionnelle

Pensez 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 si vous avez réglé des paramètres de sécurité et de confidentialité stricts, un auteur de menace peut compromettre vos comptes personnels de médias sociaux et ainsi obtenir l'accès à vos données personnelles, voire amasser des données sur les collègues faisant partie de vos contacts. Grâce à ces renseignements, ils peuvent entre autres brosser un portrait plus détaillé de votre structure organisationnelle.

Maliciels et virus

Les auteurs de menace peuvent déployer un maliciel sur un appareil ou un réseau par l'entremise d'un média social. En cliquant sur un hyperlien abrégé, une photo ou une annonce, vous pouvez ouvrir la porte à de graves cyberattaques visant les appareils et les réseaux de votre organisation. Lorsque vous utilisez vos comptes personnels au travail, évitez de cliquer sur tout ce qui vous semble suspect. Si vous pensez avoir été compromis, communiquez avec l'équipe de sécurité des TI de votre organisation.

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 menace 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 appareil et les réseaux organisationnels.

Pour en savoir plus sur le harponnage, consultez l'ITSAP.00.100, *Reconnaître les courriels malveillants*.

Mesures visant à réduire les risques liés à l'utilisation de comptes personnels de médias sociaux au travail

- Utilisez une phrase de passe ou un mot de passe unique 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.
- Mettez en œuvre l'AMF sur tous les appareils et comptes, dans la mesure du possible.
- Acceptez seulement les demandes d'amitié, d'abonnement ou de contact des personnes que vous connaissez.
- 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 personnels de médias sociaux, comme votre adresse domiciliaire ou votre numéro de téléphone. Plus vous partagez d'information, plus vous risquez d'être victime de vol d'identité.
- Passez en revue vos paramètres de confidentialité 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 toujours l'équipe de sécurité des TI de votre organisation sans tarder si vous remarquez des anormalités ou si vous soupçonnez que votre compte a été compromis.

Rappelez-vous qu'en indiquant l'endroit où vous travaillez dans votre profil et en partageant vos opinions sur les médias sociaux, votre réputation et celle de votre organisation peuvent être ternies. Tout commentaire négatif ou tout comportement en ligne inacceptable de votre part peut attirer une attention non désirée sur vous et votre lieu de travail.