

BONNES PRATIQUES SUR LES MÉDIAS SOCIAUX

La Direction du renseignement et du soutien aux opérations (DRSO) est l'équipe du ministère de la Sécurité publique du Québec chargée de faire l'analyse objective du renseignement relatif aux enjeux de sécurité et aux menaces susceptibles d'avoir des répercussions sur la sécurité de l'État québécois.

Les médias sociaux sont un endroit idéal pour obtenir des informations d'intérêt afin, notamment, d'élaborer des actions malicieuses ou une cyberattaque ciblant vous ou votre organisation. C'est pourquoi il est important d'adopter des bonnes pratiques sur les médias sociaux.

CHOISIR JUDICIEUSEMENT SES APPLICATIONS

Télécharger les applications à partir d'une boutique d'applications en ligne reconnue.

Éviter les boutiques d'applications non reconnues qui disposent d'exigences minimales en matière de confidentialité, de sécurité et de contenu. Favoriser les boutiques telles que l'App Store, Google Play Store, Microsoft Apps, etc.

Utiliser des applications sûres.

Effectuer des recherches sur la réputation et les commentaires sur l'application désirée. Vérifier la politique de confidentialité de l'application afin de valider qu'elle offre des assurances minimales en matière de sécurité.

Respecter les directives gouvernementales.

S'informer sur les applications interdites par les autorités gouvernementales québécoises sur les cellulaires et ordinateurs mis à la disposition de ses employés, notamment pour des risques de sécurité et pour la vie privée, par exemple TikTok.

SÉCURISER L'ACCÈS À VOS APPLICATIONS

Utiliser un mot de passe robuste unique pour chacun des comptes.

Activer l'authentification multifactorielle sur tous les médias sociaux qui l'offrent.

Ce type d'authentification ajoute un niveau de sécurité additionnel au processus de connexion aux comptes et appareils, rendant ainsi plus difficile la compromission d'un compte par un tiers.

Consulter les médias sociaux sur un réseau de téléphonie mobile ou un réseau Wifi sécurisé.

Les réseaux Wifi publics ou autres réseaux non sécurisés par mot de passe peuvent être plus facilement utilisés pour intercepter les données et faciliter l'installation de logiciels malveillants sur les appareils.

Installer les mises à jour des applications aussitôt disponibles.

Les mises à jour permettent d'assurer une sécurité optimale des applications. Vérifier aussi vos paramètres de confidentialité après chaque mise à jour.

1. Préférer les « phrases de passe » aux mots de passe, car elles sont plus longues et plus faciles à retenir.
2. Si l'option choisie est le mot de passe, s'assurer qu'il soit robuste :
 - Au moins 15 caractères
 - Ne se répète pas d'une application ou d'un appareil à l'autre
 - Combine les lettres majuscules et minuscules, ainsi qu'au moins un chiffre
 - Comprend un caractère spécial : lorsque placé au milieu du mot de passe, ce dernier devient significativement plus sécuritaire que lorsqu'il est placé à la fin.
3. Il est conseillé de changer vos « phrases de passe » et mots de passe régulièrement.

Informée par ses partenaires policiers et en renseignement sur les plus récentes cybermenaces, la DRSO vise à communiquer par l'entremise de ce sommaire analytique les bonnes pratiques sur les médias sociaux afin d'atténuer les risques associés à leur utilisation.

Il s'agit du dernier d'une série de trois documents sur la cybersécurité. Deux autres sommaires analytiques sont déjà disponibles sur les bonnes pratiques en cybersécurité (SA-2023-03) et pour faire face aux cybermenaces (SA-2023-04).

ADOPTER DES BONNES PRATIQUES D'UTILISATION

Séparer sa vie personnelle de sa vie professionnelle.

Créer des comptes distincts pour la vie personnelle et professionnelle. Restreindre, sur les comptes professionnels, les renseignements révélateurs sur les habitudes de vie personnelles.

Faire attention à ne pas télécharger de contenu suspect.

Se méfier des messages douteux et des liens inconnus ou suspects avant de cliquer, même ceux provenant de connaissances.

N'utiliser pas vos comptes pour vous connecter à des applications ou à des sites tiers.

Ne pas accéder à des applications ou à des sites tiers directement par l'entremise d'un compte de média social, car les applications tierces peuvent contenir des vulnérabilités facilitant le piratage des appareils.

Assurer la confidentialité de vos renseignements personnels.

Limiter l'accès aux profils à des amis côtoyés dans la réalité. Prendre également garde aux demandes d'amitié d'étrangers.

Lorsque vous êtes sur les médias sociaux, éviter de partager :

1. Des renseignements personnels : numéro de téléphone, adresse courriel, adresse de domicile, date de naissance, nom de votre partenaire et de vos enfants, nom de l'école fréquentée par vos enfants et tout autre renseignement de cette nature.
2. Des numéros d'identification personnels : numéro d'assurance sociale, de passeport, de permis de conduire, d'assurance maladie, de carte de débit/crédit, de contrat ou de dossier.
3. Des images qui révèlent des informations : avant de publier une image ou une photo, s'assurer qu'elle ne contient pas de renseignements personnels comme votre adresse de résidence ou le numéro de plaque d'immatriculation de votre véhicule.
4. La géolocalisation : éviter d'indiquer des informations de localisation en temps réel, notamment des photos, et désactiver la géolocalisation automatique des applications.
5. Les grandes nouvelles : attendre le retour avant de partager les détails des vacances ou des voyages ou les événements auxquels vous participez, éviter de partager des informations ou photos sur les achats importants ou luxueux.

VÉRIFIER LES PARAMÈTRES DE CONFIDENTIALITÉ

La gestion des paramètres de confidentialité et de sécurité vous aidera à contrôler qui voit et a accès au contenu sur vos médias sociaux.

Établir qui peut vous suivre

Public : tout le monde peut vous suivre sans nécessairement être « amis » avec vous.

Privé : permet de masquer votre compte à ceux qui n'y sont pas abonnés.

Décider qui peut voir vos publications

Vous uniquement : seul vous êtes en mesure de voir vos publications.

Amis : seules les personnes avec qui vous êtes « amis » pourront les voir.

Public : ouvert à tous, donc nul besoin d'être « amis » avec vous ou d'avoir des amis en commun pour voir l'ensemble de vos publications.

Listes personnalisées : vous pouvez créer des listes sur mesure pour gérer qui voit vos publications.

Autres paramètres à considérer

- Rendre votre liste d'amis privée et donc non visible au public.
- Empêcher les moteurs de recherche de répertorier vos profils de médias sociaux.
- Masquer les commentaires non désirés en réaction à vos publications.