BONNES PRATIQUES EN CYBERSÉCURITÉ

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.

Informée par ses partenaires policiers et en renseignement sur les plus récentes cybermenaces, la DRSO désire communiquer, par le biais de ce sommaire analytique, les bonnes pratiques en matière de protection contre les cybermenaces afin d'atténuer les risques associés principalement à l'utilisation d'appareils cellulaires et d'ordinateurs portables.

Il s'agit du premier d'une série de trois documents sur la cybersécurité. Le deuxième portera sur les cybermenaces les plus courantes visant les appareils cellulaires et les ordinateurs portables (SA-2023-04) et le troisième portera sur les bonnes pratiques sur les médias sociaux (SA-2024-01).

POUR PROTÉGER SES APPAREILS

Faire les mises à jour aussitôt que possible sur ses appareils.

Les mises à jour éliminent une grande majorité des vulnérabilités et des logiciels malveillants.

Se méfier des pièces jointes ou des liens reçus par courriel ou message texte.

Se questionner avant de cliquer, particulièrement si l'envoi ou l'expéditeur est inhabituel.

Utiliser des **mots de passe robustes**.

Éviter de se connecter aux réseaux Wifi gratuits/publics.

Utiliser les données de son forfait cellulaire sur son appareil.

Éviter de se connecter aux bornes de recharge USB publiques.

Privilégier l'utilisation d'une prise électrique ou d'une batterie externe pour recharger son appareil.

Verrouiller ses appareils lorsqu'ils ne sont pas utilisés.

LES MOTS DE PASSE ROBUSTES…

- Sont longs : Au moins 15 caractères.
- Sont uniques : Ils ne sont pas réutilisés d'une application ou d'un appareil à l'autre.
- Comprennent un caractère spécial : Lorsque placé en milieu de mot de passe, ce dernier devient significativement plus sécuritaire que lorsqu'il est placé à la fin.

Au besoin, utiliser un gestionnaire de mots de passe fiable. Exemples : NordPass ou Bitwarden.

POUR PROTÉGER SES INFORMATIONS PERSONNELLES ET PROFESSIONNELLES

Sécuriser ses communications sensibles.

Éviter d'utiliser les SMS. Les communications sensibles de personnes à personnes peuvent être sécurisées via une application de chiffrement reconnue, comme Signal.

Restreindre ses profils de médias sociaux.

Limiter l'accès à ses profils aux personnes que vous connaissez dans la réalité et éviter d'indiquer des localisations en temps réel.

Sauvegarder dans l'espace infonuagique (cloud) uniquement le contenu autorisé.

Éviter d'y enregistrer le contenu personnel qui pourrait contenir des logiciels malveillants ou des données compromises afin de prévenir qu'ils soient réinstallés lors d'une restauration de sauvegarde.

Séparer sa vie personnelle de sa vie professionnelle.

Éviter d'utiliser le cellulaire ou l'ordinateur du travail pour consulter des applications ou sites personnels.

POUR PROTÉGER SES CONVERSATIONS CONFIDENTIELLES

Laisser les appareils électroniques à l'extérieur des salles lors de réunions sensibles.

Éviter tout risque d'être écouté et/ou localisé.

Activer le mode avion de l'appareil, puis le placer dans un sac Faraday ou ne pas conserver l'appareil avec soi.

POUR SE PROTÉGER LORS DE DÉPLACEMENTS

Ne jamais connecter de clés USB trouvées.

Éviter autant que possible l'utilisation des clés USB. Privilégier l'envoi par courriel ou le partage des répertoires.

Se méfier des traceurs qui peuvent être placés sur son véhicule.

Les traceurs de style « AirTag » peuvent émettre une localisation.

Se méfier du clonage des clés automatiques et des cartes d'accès.

Des dispositifs permettent de copier le signal émis par une clé automatique d'un véhicule ou une carte d'accès depuis une distance allant jusqu'à 20 m.

Ne jamais connecter son cellulaire au système d'une voiture de location.

Des données sont conservées dans la mémoire du véhicule.

Ne jamais utiliser des fils de recharge inconnus.

Les fils pourraient être compromis et permettre la consultation ou le vol des données de son appareil.

En tout temps

Demeurer vigilant aux comportements inhabituels de l'appareil.

Des fenêtres inhabituelles ou une réduction anormale de l'efficacité de la batterie peuvent constituer des signes de compromission. En cas de doute, ne pas hésiter à recourir à sa direction des services informatiques afin d'obtenir des indications spécifiques sur la marche à suivre.