SOMMAIRE ANALYTIQUE

DIRECTION DU RENSEIGNEMENT ET DU SOUTIEN AUX OPÉRATIONS

1er septembre 2023

NON CLASSIFIÉ

BONNES PRATIQUES POUR FAIRE FACE AUX CYBERMENACES

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 visant à se prémunir contre les deux cybermenaces les plus courantes visant les appareils cellulaires et les ordinateurs portables.

Il s'agit du deuxième d'une série de trois documents sur la cybersécurité. Un premier sommaire analytique est déjà disponible sur les bonnes pratiques en cybersécurité (SA-2023-03). Le dernier sommaire analytique de cette série portera sur les bonnes pratiques sur les médias sociaux (SA-2024-01).

VECTEUR DE MENACE : MÉDIAS SOCIAUX

Les médias sociaux constituent un environnement propice pour les auteurs de cybermenaces souhaitant élaborer une attaque contre vous ou votre organisation, en raison de la profusion de renseignements personnels que l'on peut retrouver sur les différentes plateformes.

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

Les réseaux Wifi publics ou mobiles non sécurisés par mot de passe peuvent être utilisés pour intercepter les données et les renseignements et injecter des logiciels malveillants dans les appareils connectés.

Revoir régulièrement les paramètres de confidentialité.

Utiliser les paramètres de confidentialité et de sécurité pour contrôler qui peut vous suivre et limiter l'accès à vos profils aux personnes que vous connaissez dans la réalité. Pour ce faire, désactiver les réglages par défaut qui rendent vos comptes publics.

Restreindre les renseignements révélateurs sur votre vie personnelle et professionnelle.

Faire attention à ce que vous publiez. Certains renseignements peuvent aider les auteurs de cybermenaces à recueillir des informations sur vous ou votre employeur.

RANÇONGICIELS

Les rançongiciels sont des logiciels malveillants qui, lorsqu'ils infectent un ordinateur ou un téléphone cellulaire, peuvent verrouiller l'accès aux fichiers ou au système. Ils peuvent également s'en prendre aux systèmes de sauvegarde et de restauration du système et se propager aux ordinateurs et appareils connectés au même réseau. Une fois qu'un tel logiciel est exécuté, une demande de rançon, payable par monnaie virtuelle telle que le bitcoin, apparaît à l'écran en échange de la clé de déchiffrement.

Effectuer les mises à jour aussitôt que possible.

La plupart des rançongiciels exploitent des vulnérabilités pour lesquelles il existe déjà des correctifs.

Sécuriser les communications à distance.

Utiliser un réseau Wifi sécurisé ou de téléphonie mobile. Favoriser des outils d'accès à distance sécurisés tels que des « VPN », en utilisant des mots de passe robustes.

Instaurer une procédure de sauvegarde périodique.

Mettre en place un plan de sauvegarde informatique visant à protéger vos données, conformément aux recommandations des directions des services informatiques.

Ne pas payer la rançon.

Payer la rançon ne garantit pas la récupération des données ni qu'elles ne soient pas rendues publiques et incite d'autres criminels à se lancer dans ce type d'activités.

Si vous êtes victimes d'un rançongiciel ou d'hameçonnage, contacter le plus rapidement possible votre direction des services informatiques afin d'obtenir des indications spécifiques sur la marche à suivre.

HAMEÇONNAGE

L'hameçonnage se produit lorsqu'un auteur de cybermenaces se fait passer pour une personne de confiance par l'entremise d'un courriel, d'un message texte ou d'un appel téléphonique pour tenter d'obtenir frauduleusement des renseignements ou l'accès à des systèmes. Une telle attaque réussie peut avoir de graves conséquences : vol de données personnelles, d'informations d'identification, d'informations bancaires, usurpation d'identité, fraude, vol de documents sensibles ou blocage de l'accès à ceux-ci, etc.

PAR COURRIEL

Éviter l'ouverture de pièces jointes, le téléchargement de fichiers ou de cliquer sur un lien lorsque vous ne connaissez pas l'expéditeur.

Savoir détecter les signes d'une attaque par hameçonnage :

- Provient d'une personne ou d'une organisation inconnue;
- Provient d'une personne ou d'une organisation connue, mais avec un nom de domaine inconnu (nom unique qui apparaît après le signe @ dans une adresse courriel);
- Exprime un niveau inhabituel d'urgence dans sa communication;
- Contient parfois des erreurs telles que des noms mal orthographiés, des termes ou expressions organisationnels mal utilisés ou des logos mal représentés;
- Communication motivée par un avantage financier ou une raison incongrue.

PAR SMS

Ne pas répondre à un message texte suspect et ne pas cliquer sur les liens pouvant s'y trouver.

Rechercher sur Internet le numéro de téléphone et les propos dans le message pour vérifier si d'autres personnes ont reçu des messages similaires.

En cas de doute, communiquer directement avec l'expéditeur par un autre moyen que vous connaissez comme étant sûr et demander si le message que vous avez reçu est légitime.

PAR TÉLÉPHONE

Se méfier des appels téléphoniques non sollicités vous demandant des renseignements personnels ou sensibles.

Ne jamais donner votre numéro d'assurance sociale, vos mots de passe ou autres informations confidentielles par téléphone. Ne pas partager d'informations qui pourraient révéler une question de sécurité.

Ne jamais faire d'opérations précipitées sur vos appareils.

Dans l'immédiat, n'effectuer aucune opération ou manipulation à la demande de votre interlocuteur, comme un paiement par téléphone ou vous connecter à vos comptes personnels.

Vérifier les appels téléphoniques suspects.

En cas de doute, raccrocher immédiatement et rappeler la personne ou l'organisation par le numéro publié sur le site web de son service à la clientèle.

Sécurité publique Québec