Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

PRATIQUES EXEMPLAIRES EN CYBERSÉCURITÉ POUR LA COVID-19

Le Centre pour la cybersécurité a constaté que des auteurs malveillants se servent de plus en plus du coronavirus (COVID-19) pour mener des campagnes d'hameçonnage et d'escroquerie liées à des maliciels.

L'Agence de la santé publique du Canada dirige la réponse à la COVID-19 en collaboration avec les responsables et les organismes de la santé publique d'un bout à l'autre du Canada. Pour obtenir les renseignements les plus récents sur la COVID-19, veuillez consulter la page Web du gouvernement du Canada concernant la mise à jour sur l'éclosion.

MÉFIEZ-VOUS DES TROMPERIES

À mesure que l'inquiétude du public à l'égard de la COVID-19 s'accroît, le nombre de tentatives d'hameçonnage faisant référence au virus augmente. L'hameçonnage consiste à envoyer des courriels de masse qui semblent provenir d'une source légitime, mais qui contiennent une pièce jointe infectée ou un lien malveillant. Les courriels sont rédigés de manière à inciter les destinataires à ouvrir une pièce jointe ou à cliquer sur un lien pour permettre aux auteurs de menaces d'obtenir des justificatifs d'identité personnels ou d'accéder sans autorisation à un système informatique. Dans certains cas récents, des auteurs malveillants se sont fait passer pour divers organismes de santé dans leurs tentatives d'hameçonnage.

Les auteurs de cybermenace saisissent rapidement l'occasion de profiter d'événements fortement médiatisés, surtout si ces événements soulèvent des inquiétudes ou des préoccupations.

COMMENT VOUS PROTÉGER

Voici quelques mesures à prendre afin de protéger votre appareil contre les maliciels :

Courriels malveillants :

- Assurez-vous que l'adresse ou la pièce jointe est liée au contenu du courriel.
- Assurez-vous de connaître l'expéditeur du courriel.
- Vérifiez s'il y a des coquilles.
- Utilisez un logiciel antivirus ou antimaliciel sur vos ordinateurs.

Pièces jointes malveillantes :

- Assurez-vous que l'adresse courriel de l'expéditeur comprend un nom d'utilisateur et un nom de domaine valides.
- Méfiez-vous si le ton de l'expéditeur est urgent.
- Si vous ne vous attendiez pas à recevoir une pièce jointe, vérifiez auprès de l'expéditeur.

Sites Web malveillants :

- Assurez-vous que les URL sont bien épelées.
- Tapez l'URL directement dans la barre de recherche au lieu de cliquer sur le lien fourni.
- Si vous devez cliquer sur un hyperlien, pointez votre curseur sur le lien pour vérifier qu'il vous dirigera bel et bien vers le site Web indiqué.

4 MOYENS PRATIQUES DE RENFORCER VOTRE CYBERSÉCURITÉ

- Utilisez des mots et des phrases de passe uniques et complexes
- Mettez à jour vos ordinateurs, vos applications et vos appareils mobiles
- Stockez vos données de façon sécurisée et sachez comment récupérer les copies de sauvegarde
- Sécurisez vos comptes de médias sociaux et de courriel

Êtes-vous prêt?

Mesures de sécurité des TI visant à protéger votre organisation