PEOPLE RESOURCES

Comment reconnaître l'hameçonnage lié à la COVID-19

Association des banquiers canadiens

Les criminels essaient de tirer profit de la pandémie créée par la COVID-19, nouvelle maladie au coronavirus. Des courriels frauduleux sont envoyés afin d'amener le destinataire à révéler des renseignements personnels ou à cliquer sur des liens et des pièces jointes contenant des maliciels.

Les courriels semblent authentiques, avec le logo et le marquage de l'Organisation mondiale de la Santé ou d'une autre agence gouvernementale ou de santé publique. Dans une variation de cette escroquerie, des criminels appellent les citoyens soit pour demander des dons, soit pour leur offrir des tests de laboratoire. FRAUDULEUX dans les deux cas.

Comment déceler une escroquerie

Dans une fraude par hameçonnage, les criminels essaieront de vous inciter à leur communiquer vos renseignements personnels - notamment le numéro de votre carte de crédit - ou à installer un maliciel sur votre ordinateur ou appareil mobile. Vous pouvez adopter des mesures simples pour éviter de vous retrouver victime de cette fraude.

- **Méfiez-vous** – Les courriels frauduleux semblent souvent provenir de la part d'une vraie organisation. Vous devrez vous douter de tout message électronique où on prétend vous donner des renseignements sur la santé ou bien dans lequel on sollicite des dons pour les Canadiens affectés par la COVID-19. Évitez les maliciels et n'utilisez ni les numéros de téléphone ni l'adresse électronique ou du site Web inclus dans le message. Cherchez plutôt ces coordonnées en ligne ou dans votre carnet d'adresses. Consultez les renseignements à propos de la COVID-19 sur le site Web de l'Agence de la santé publique du Canada ou sur celui de l'agence de santé publique de votre province.
- **Soyez vigilant** – N'envoyez jamais par courriel vos renseignements personnels ou financiers.
- **Vérifiez l'adresse de l'expéditeur** – Le nom dans le champ de l'expéditeur peut sembler celui de l'organisation, mais l'adresse électronique qui y est rattachée ne l'est pas nécessairement. Pour vérifier, il suffit de placer votre curseur au-dessus du nom, sans cliquer.
- **Ne cliquez jamais sur des pièces jointes ou des liens douteux** – Les courriels hameçons contiennent souvent des liens qui ont l'air légitimes, mais conduisent plutôt à des sites frauduleux. Là également, il suffit de placer le curseur au-dessus du lien pour voir l'adresse du site vers lequel il mène. Par ailleurs, n'ouvrez jamais des pièces jointes auxquelles vous ne vous attendez pas.
- **Protégez vos appareils** – Comme toujours, assurez-vous que vos ordinateurs personnels sont bien protégés. Vous devez toujours avoir les plus récentes versions des logiciels antivirus, anti-espion et antipourriel.

Si vous recevez un courriel hameçon, vous devez le signaler et le supprimer. Lorsque vous signalez la fraude à l'organisation qui a été usurpée, vous contribuez à limiter le nombre de futures victimes. Pour ce faire, vous devez envoyer le courriel reçu comme pièce jointe à l'organisation en question.

Le Centre antifraude du Canada a dressé une liste des arnaques signalées en lien avec la COVID-19.

PEOPLE RESOURCES

Le gouvernement du Canada met à la disposition des citoyens des renseignements sur la COVID-19, ainsi qu'un numéro de téléphone sans frais et une adresse de courrier électronique : https://www.canada.ca/en/public-health/services/diseases/2019-novel-coronavirus-infection.html

Veuillez consulter votre partenaire des ressources humaines si vous voulez suivre le cours en ligne offert sur Litmos à propos de la sécurité de l'information de Black & McDonald. Il vise à vous faire connaître les principes de la cybersécurité et les précautions nécessaires pour protéger l'information, les ressources de l'entreprise et les gens des accès non autorisés et des attaques. Chaque employé a son rôle à jouer dans la protection de l'information et des données de notre entreprise. Le cours est d'une durée d'environ 20 minutes.