CYBER-RESPONSABILITÉ

Comment vous protéger des arnaques technologiques liées à la COVID-19

VICTOR

Au cours de cette période sans précédent, des millions de Canadiens et de Canadiennes pratiquent la distance physique (sociale) et travaillent de la maison. Ces pratiques sont actuellement la « nouvelle norme » pour se protéger de la COVID-19.

Cependant, en travaillant de la maison, nous sommes devenus plus vulnérables aux arnaques technologiques liées à la COVID-19. Cette pandémie a créé un environnement parfait pour les cyberfraudeurs et les cybercriminels qui cherchent à tirer profit de nos émotions (peur, inquiétude, sympathie) pour leur propre gain personnel ou monétaire. Que nous soyons sur nos ordinateurs, nos portables, nos tablettes ou nos téléphones cellulaires, nous devons être sur nos gardes.

Voici cinq exemples d'arnaques technologiques liées à la COVID-19 que vous pourriez rencontrer, ainsi que des conseils sur la façon de vous protéger de ces arnaques avant qu'elles ne se produisent.

Courriel hameçon

Arnaque 1

Vous recevez un courriel dont l'objet est : « Mise à jour relative à la COVID-19 » ou « urgent » avec un lien qui vous dirige vers une supposée page de connexion Microsoft, vous demandant ensuite de vous connecter pour accéder à de l'information essentielle. Il s'agit d'un courriel frauduleux d'hameçonnage. L'arnaqueur veut recueillir votre mot de passe et voler votre argent et votre identité. Une telle arnaque peut apparaître comme si elle venait d'une autorité de santé publique reconnue (p. ex. Santé Canada), d'un bureau du gouvernement (p. ex. gouvernement du Canada), ou même d'un collègue, d'un ami ou d'un membre de la famille.

Conseil

Un courriel dont l'information importante est envoyée sous forme de pièce jointe seulement et dont le corps contient peu ou pas de texte est probablement une arnaque. Si un organisme de santé publique veut vous mettre au courant d'informations importantes relatives à la COVID-19, il vous le dira simplement dans le corps du courriel ou il vous enverra une lettre par courrier ordinaire.

Ne « cliquez » pas sur un lien sans vous être tout d'abord assuré qu'il s'agit d'une adresse valide. Les arnaqueurs sont de plus en plus sophistiqués et peuvent créer des courriels convaincants qui nous poussent à agir. Méfiez-vous des courriels ou des textes que vous ne vous attendiez pas à recevoir, principalement ceux qui contiennent des liens et des pièces jointes de la part d'expéditeurs inconnus ou suspects. Si vous n'êtes pas certain que le courriel ou le texte a été envoyé par une personne ou une entreprise connue, communiquez directement avec cette personne ou cette entreprise pour vous assurer de la véracité du message.

Pirate informatique

Arnaque 2

Vous naviguez sur Internet tandis que vous êtes sur le réseau de votre entreprise et visitez un site Web non reconnu qui contient supposément de l'information relative à la COVID-19. Vous cliquez sur un lien vous menant à cette information, provoquant ainsi l'infection du réseau de votre entreprise par un virus rançonneur qui rend le réseau et les données de votre entreprise inaccessibles. Le virus provoque également une panne du réseau et des systèmes de votre entreprise. Maintenant, aucun employé de votre entreprise ne peut accéder à son ordinateur et aux systèmes et vous faites face à des demandes de rançon.

Conseil

Soyez prudent lorsque vous naviguez sur Internet et assurez-vous que les sites Web sont légitimes et des sources fiables. Prêtez attention au nom du domaine. Les arnaqueurs peuvent imiter les entreprises connues en apportant de petites modifications au nom officiel de l'entreprise (p. ex. Ontari00.com) pour vous piéger. Veuillez donc revérifier la barre d'adresse du site Web pour tout d'abord vous assurer de son exactitude avant de visiter un site Web. De plus, avant d'entrer tout renseignement personnel, assurez-vous que l'adresse du site Web est sécuritaire et qu'elle utilise le cryptage. Vous pouvez le faire en vérifiant que l'URL débute par « https » (et se termine avec un « s ») comparativement aux sites Web non sécurisés qui débutent par « http ». N'entrez jamais de renseignements personnels sur les sites Web non sécurisés. Certains navigateurs, notamment Google, Mozilla ou Internet Explorer, peuvent vous mettre en garde contre des sites Web suspects ou non sécurisés. Recherchez des erreurs de grammaire ou d'orthographe, lesquelles pourraient être des indices qu'un site Web a été créé rapidement et qu'il est frauduleux. Les entreprises légitimes possèdent des sites Web professionnels ayant du contenu qui respecte la grammaire.

Pour atténuer les attaques potentielles à votre réseau informatique, assurez-vous également d'avoir un système de détection d'intrusion, un anti-virus et un logiciel anti-vol en place et d'observer des protocoles réguliers de sauvegarde. N'utilisez qu'une connexion sans fil sécurisée avec un logiciel de sécurité et de protection en place. N'utilisez pas de réseaux sans fil ouverts ou accessibles publiquement lorsque vous travaillez sur votre portable ou sur tout autre appareil technologique.

Arnaque 3

Vous recevez un message texte sur votre téléphone cellulaire de ce qui semble être un organisme de soutien d'urgence en réponse à la COVID-19, prétendant vous avoir envoyé des fonds de secours pour vous aider pendant cette crise financière. Il s'agit d'un message texte frauduleux nommé « hameçonnage par message texte ».

Conseil

Le premier ministre, Justin Trudeau, a émis un avertissement concernant les messages textes frauduleux qui tentent d'attirer les Canadiens et les Canadiennes sans méfiance avec des messages d'aide relatifs à la COVID-19 (consultez CBC news en anglais : « Trudeau warns of COVID-19 text scam exploiting new emergency benefit program »). Protégez-vous et méfiez-vous des messages textes de la part d'expéditeurs inconnus ou suspects. En fait, ne cliquez sur aucun lien à moins d'avoir un motif suffisant pour lui faire confiance ou à moins que ce soit un site Web bien connu d'un organisme établi (p. ex. gouvernement du Canada, Organisation mondiale de la Santé, etc.).

Si vous n'êtes pas certain que le site Web que vous visitez est lié à un organisme établi ou reconnu, effectuez des recherches. Copiez le lien ou l'adresse du site Web de l'organisme en question directement dans votre navigateur Web pour vous assurer qu'il est légitime. Si vous n'attendiez pas de message texte, il s'agit probablement d'un message texte frauduleux et d'une tentative d'infecter votre téléphone cellulaire ou appareil avec un virus, rendant ainsi votre téléphone ou votre appareil inaccessible. Le message texte pourrait également être une tentative d'accès à des renseignements sensibles non autorisés. Ne répondez pas au message texte et supprimez-le immédiatement.

Arnaque 4

Vous recevez un appel sur votre téléphone, supposément de votre administration municipale, sollicitant des dons pour aider à combattre la crise de la COVID-19. En tant qu'entreprise, vous pouvez également recevoir des appels de la part d'arnaqueurs qui tentent d'exploiter votre vulnérabilité en raison des retombées financières de la crise, en vous offrant des fournitures de premiers soins ou un prêt d'urgence.

Conseil

C'est une forme de fraude liée à l'ingénierie sociale ou d'arnaque nommée « hameçonnage vocal ». Il s'agit d'une technique de fraude qui amène par la ruse les individus à divulguer leurs renseignements financiers ou personnels. En fait, cela s'est produit lorsque des fraudeurs se faisant passer pour des employés de la ville de Brandon ont sollicité des dons (consultez l'article du CBC news en anglais : « Fraudsters pretending to represent city staff in COVID-19 phone scam: Brandon police »). Ne révélez pas vos renseignements personnels ou financiers aux appelants non sollicités. Raccrochez et appelez directement l'organisme ou l'organisation de bienfaisance pour vérifier la validité de l'appel avant de fournir tout renseignement. Cette étape de vérification supplémentaire vous aidera à vous protéger contre des pertes financières.

De plus, assurez-vous que vos employés sont conscients de ces arnaques afin qu'ils puissent les éviter. Cependant, si vous avez été victime d'une telle arnaque, communiquez avec le Centre antifraude du Canada ou avec votre police locale. Si vous possédez une police d'assurance liée à la cyber-responsabilité, signalez cette arnaque téléphonique à votre compagnie d'assurance.

Attaque de l'intercepteur

Arnaque 5

En raison de la crise liée à la COVID-19, vous travaillez maintenant de la maison et décidez de répondre aux questions pressantes des clients avec votre courriel personnel afin de gagner du temps. Puisque votre courriel personnel n'est pas crypté, un arnaqueur peut accéder à vos courriels et être au courant de renseignements sensibles et confidentiels. L'arnaqueur est alors en mesure d'utiliser ces renseignements pour commettre un vol d'identité sur vos clients. Par conséquent, vous faites face à une possible réclamation de responsabilité envers les tiers. Et ce n'est pas tout. Votre compagnie d'assurance ne paiera pas votre réclamation puisque vous n'utilisiez pas votre réseau d'entreprise sécurisé en travaillant.

Conseil

N'utilisez que des réseaux protégés de l'entreprise lorsque vous travaillez de la maison. Évitez d'utiliser des courriels personnels puisqu'ils sont hors du contrôle de votre département des technologies informatiques, et qu'ils n'ont pas les mêmes protocoles de sécurité rigoureux. Les entreprises utiliseront habituellement les RPV/VPN, l'authentification à deux facteurs ou l'authentification à facteurs multiples (AFM) en plus de la sécurité supplémentaire afin d'accéder à leurs réseaux de façon sécuritaire.

Les courriels personnels peuvent non seulement vous exposer aux « attaques de l'intercepteur », mais ils peuvent également exposer involontairement des renseignements sensibles dans vos courriels qui peuvent être facilement accessibles aux individus qui ne sont pas dignes de confiance (« acteurs de mauvaise foi ») ou des pirates informatiques. Vous pouvez également violer les politiques de l'entreprise en utilisant votre courriel personnel et vous retrouver sans assurance en cas de réclamation. Enfin, en toutes circonstances, assurez-vous que votre nom d'utilisateur et votre(vos) mot(s) de passe ne sont pas faciles à deviner pour un arnaqueur. Mettez régulièrement à jour vos mots de passe et utilisez des mots de passe et des noms d'utilisateur qui consistent en une combinaison complexe de lettres, de nombres et de symboles. Évitez d'utiliser des noms et des nombres communs (p. ex. votre nom, votre date de naissance, 123, etc.).

Conseils supplémentaires lorsque vous travaillez de la maison pendant la crise de la COVID-19

- Ne copiez pas de renseignements relatifs au travail vers des appareils technologiques personnels (p. ex. téléphone personnel, ordinateur personnel, stockage en ligne personnel, etc.).
- Coupez le son ou arrêtez tout assistant numérique, notamment Alexa, Google Home, etc. puisqu'ils enregistrent constamment les conversations à proximité.
- Protégez vos renseignements personnels lors de vidéo conférence sur des plateformes comme Zoom ou Skype en rendant la rencontre privée afin d'éviter que des « acteurs de mauvaise foi » s'y introduisent. De plus, limitez le partage des renseignements pour protéger les renseignements sensibles.
- Ne laissez pas les membres de la famille ou les amis utiliser l'équipement fourni par votre entreprise (p.ex. portable, téléphone cellulaire, etc.).
- N'utilisez pas de courriel personnel, de sites de partage de fichiers, de médias sociaux ou d'autres systèmes qui ne sont pas approuvés et sécurisés par votre entreprise.
- Effectuez régulièrement des audits et des tests de sécurité sur votre ordinateur et vos systèmes.
- Mettez un plan en place en cas d'arnaque technologique ou de cyberattaque.
- Si vous possédez ou dirigez une entreprise, assurez-vous qu'elle a une assurance liée à la cyber-responsabilité en place.

Pour plus d'informations, visitez assurancevictor.ca ou consultez les ressources supplémentaires suivantes :

- Assurance contre les cyber-risques de Victor (auparavant ENCON)
- Ressources sur la COVID-19
- Infographie : « Journée typique dans la vie d'un propriétaire »
- Vidéo animée : « Une journée dans la vie d'un propriétaire d'entreprise dans un cybermonde »

#COVID-19 #ArnaquesTechnologiques #LaMenaceEstRéelle #SoyezPrudent