La fraude par courriel et comment l’éviter

[Musique douce.]

[Le logo de Gestion privée CIBC.]

[La fraude par courriel et comment l’éviter.]

[Une femme travaille sur un ordinateur portable.]

La fraude par courriel est courante et nous concerne tous. Cette vaste industrie criminelle a détourné plus de 4 milliards de dollars.

[Un nombre animé passe d’environ 3 900 000 000 $ à environ 4 200 000 000 $]

[Source : FBI (Federal Bureau of Investigation), rapport 2020 sur la criminalité sur Internet (2020 Internet Crime Report)]

La fraude se produit souvent d’une de ces deux façons :

En premier lieu, les faux comptes de courriel.

[Photo d’un homme regardant une tablette]

[1. Les faux comptes de courriel.]

Un fraudeur crée un faux compte de courriel et se fait passer pour une personne ou entité fiable.

[Icône de tête de voleur avec une flèche pointant vers une enveloppe dont sort une feuille où figure la tête du voleur.]

Son but est l’accès à vos renseignements personnels et à votre argent.

[Une boîte de réception de courriel. Un courriel est en surbrillance : l’expéditeur est « Agence du revenu » et l’objet est : « Urgent : Veuillez confirmer vos identifiants de connexion ».]

Vous pourriez par exemple recevoir un message de Virement *Interac* entrant.

[Un message texte sur un téléphone : « Bonjour Cindy, suivez le lien pour accepter votre virement électronique : bit.ly/1sNMQw »]

Vous suivez le lien vers une page Web frauduleuse. Elle semble authentique, mais a été créée par le fraudeur. Vous entrez votre numéro de carte et votre mot de passe. Le fraudeur peut maintenant contourner la sécurité en se faisant passer pour VOUS.

[Une page d’accueil de site Web bancaire. Dans le champ Numéro de carte vide, un numéro de carte s’affiche. Dans le champ Mot de passe vide, un mot de passe s’affiche.]

D’autres fraudes courantes exploitent les livraisons de colis, cartes-cadeaux et locations à temps partagé.

[Livraisons de colis
Cartes-cadeaux
Locations à temps partagé.]

En deuxième lieu, il y a la prise de contrôle d'un compte de courriel.

[Photo d'une femme qui regarde un ordinateur]

[2. Prise de contrôle d'un compte de courriel de confiance]

Les fraudeurs s'emparent alors d'un compte réel. Cela fait, ils peuvent envoyer des courriels de ce compte et se faire passer pour son détenteur.

[Icône de tête de voleur et icône d'ordinateur de bureau. L'icône de tête de voleur se superpose à l'icône d'ordinateur de bureau. Des flèches suivies d'enveloppes dont sort une feuille où figure le symbole « @ » commencent à sortir de l'ordinateur de bureau.]

Comme ils ont accès aux courriels du détenteur, ils peuvent utiliser des renseignements confidentiels pour rendre l'arnaque plus authentique. La prise de contrôle de compte de courriel peut arriver à tout le monde, même à des professionnels fiables.

[La prise de contrôle d'un compte de courriel de confiance peut faire des victimes partout]

Par exemple : vous achetez un chalet et le compte de courriel de votre avocat est compromis par un fraudeur, qui lit vos courriels passés pour obtenir des renseignements sur votre achat.

[Une boîte de réception de courriel. Un courriel est en surbrillance : l'expéditeur est « Cindy Smith » et l'objet est : « Transfert de fonds pour l'achat du chalet de Gold Lake ».]

[Texte du courriel. L'objet est « RE : Achat du chalet de Gold Lake ». L'expéditeur du courriel est Brendan Jones, brendan.jones@realestatelawyers.com.]

Se faisant passer pour votre avocat, il vous envoie un message indiquant où envoyer le virement avant la date de clôture. Croyant le message authentique, vous demandez à VOTRE BANQUE de virer les fonds au fraudeur. Ils deviennent presque instantanément irrécupérables.

[Icône de tête de voleur dans un ordinateur de bureau, au-dessus duquel se trouve la mention « Avocat » (fraudeur). Une flèche et une enveloppe contenant une feuille où figure le symbole « @ » sortent de l'ordinateur de bureau. Une autre flèche sort de cette enveloppe et pointe vers une icône de personne au-dessus de laquelle se trouve la mention « Vous ». Une flèche sort de l'icône de personne et pointe vers une icône de téléphone. Une flèche sort de l'icône de téléphone et pointe vers une icône de banque au-dessus de laquelle se trouve la mention « Votre banque ». Une flèche sort du bas de l'icône de la banque et pointe vers la gauche, en direction de l'icône d'ordinateur de bureau. Des icônes de dollars commencent à sortir de la flèche en direction de l'icône de l'ordinateur de bureau, puis y disparaissent.]

Voici quelques conseils pour éviter une telle situation :

[Conseil nº 1

Faites un suivi par téléphone]

- Confirmez les instructions par téléphone auprès du destinataire du virement (votre avocat dans cet exemple) et appelez aussi VOTRE BANQUE.

[Icône de tête de voleur dans un ordinateur de bureau, au-dessus duquel se trouve la mention « Avocat » (fraudeur). Une flèche et une enveloppe contenant une feuille où figure le symbole « @ » sortent de l'ordinateur de bureau. Une autre flèche sort de cette enveloppe et pointe vers une icône de personne au-dessus de laquelle se trouve la mention « Vous ». Une flèche sort du bas de l'icône de personne et pointe vers une icône de téléphone plus bas. Une flèche sort du bas de l'icône de téléphone et pointe vers une icône de personne plus bas, au-dessus de laquelle se trouve la mention « Votre avocat ».

Une autre flèche sort de l'icône de personne portant la mention « Vous » et pointe vers une icône de téléphone. Une flèche sort de l'icône de téléphone et pointe vers l'icône de banque portant la mention « Votre banque ».]

- C'est vraiment important pour les courriels sur des opérations d'un montant élevé. Assurez-vous d'utiliser le numéro de téléphone que VOUS avez noté et non celui contenu dans le courriel, puisque le fraudeur pourrait l'avoir modifié. Cet appel pourrait valoir des milliers, voire des millions de dollars.

[Illustration d'un téléphone cellulaire. L'écran affiche les contacts, y compris le nom de « Brendan (avocat) », suivi de son numéro de téléphone en surbrillance. Le texte du courriel s'affiche à côté du téléphone. L'aspect important est la ligne en surbrillance indiquant : « Pour confirmer, veuillez appeler au 516 284-3617. »]

[Conseil nº 2
Utilisez des mots de passe forts]

- Utilisez des mots de passe FORTS. Bien des gens utilisent des mots de passe très faibles.
  – Par exemple, 24 % utilisent « Qwerty », « mot de passe » ou « 123456 » comme mot de passe.
  – Évitez les mots de passe qui suivent une structure simple.
  – Utilisez des chiffres aléatoires et, lorsque cela est possible, rendez aléatoires les caractères en utilisant des lettres et des caractères spéciaux.
  – Enfin, une PHRASE de passe protège mieux qu'un MOT de passe.

[Écran d'ouverture de session du personnage fictif Cindy Smith. Dans le champ Mot de passe plusieurs mots de passe différents s'affichent successivement, en synchronisme avec la voix hors champ.]

[Conseil nº 3
Créez des mots de passe uniques]

- Créez des mots de passe UNIQUES, SURTOUT pour votre compte de courriel. Deux personnes sur trois utilisent le même mot de passe pour TOUS leurs comptes. C'est à éviter, car la première cause de compromission des courriels est la réutilisation de mot de passe.

- Gardez vos mots de passe secrets; ne les envoyez à personne, ni même à votre adresse courriel.

[Quatre écrans d'ouverture de session différents du personnage fictif Cindy Smith. Le même mot de passe figure sur tous les écrans.]

[Gardez vos mots de passe secrets]

Songez à utiliser un gestionnaire de mots de passe. Vous aurez des mots de passe uniques pour chaque compte, sans le stress de devoir les mémoriser.

[Conseil nº 4
Réfléchissez avant de réagir!]

- RÉFLÉCHISSEZ avant de réagir. Si vous doutez de la fiabilité d'un lien, trouvez vous-même le site Web pour en confirmer l'authenticité.

[Une page d'accueil de site Web bancaire.]

- Méfiez-vous des expressions comme « Opération inhabituelle détectée » ou « Connectez-vous ».

[Une boîte de réception de courriel. Un courriel est en surbrillance : l'expéditeur est « Agence du revenu » et l'objet est : « Opération inhabituelle détectée ».]

- Les courriels malveillants invoquent l'urgence pour vous inciter à agir rapidement. N'oubliez pas : La Banque CIBC ne vous enverra JAMAIS de courriel demandant vos mots de passe, votre numéro d'assurance sociale ou d'autres renseignements confidentiels.

[Conseil nº 5
N'ouvrez JAMAIS les pièces jointes si vous n'en attendiez pas]

- N'ouvrez JAMAIS les pièces jointes si vous n'en attendiez pas de la part de l'expéditeur.

Nous espérons que vous comprenez mieux les fraudes par courriel et comment les éviter. La Banque CIBC demeure vigilante et très alerte.

[Montage de diverses photos où différentes personnes travaillent à l'ordinateur, regardent une tablette ou parlent au téléphone.]

Nous faisons tout en notre pouvoir pour protéger nos clients. Avec votre aide, nous pouvons travailler ensemble pour créer l'environnement le plus sécuritaire possible pour vous et vos actifs.

[Le logo de Gestion privée CIBC.]