

Escroqueries pendant la pandémie de la COVID-19

Au cours des derniers mois, la pandémie de la COVID-19 a été la principale préoccupation de nombreuses familles et entreprises. Elle a également fait la une des journaux dans le monde entier et l'objet de maintes spéculations quant à la nature du virus et aux moyens de limiter son impact. Alors que de nombreuses familles et entreprises ont vu leurs revenus diminuer en raison de la pandémie, les fraudeurs ont saisi l'occasion d'étendre leurs activités malveillantes au détriment des Canadiens non méfiant. Selon le Centre antifraude du Canada, entre le 6 mars et le 1^{er} mai 2020, 766 fraudes liées à la Covid-19 ont été signalées au Canada, faisant 188 victimes et engendrant la perte de 1,2 million de dollars.

Au début du mois de mai, la police du centre de l'Okanagan a lancé un avertissement aux habitants à propos d'une nouvelle escroquerie dans la région. La GRC de Kelowna a indiqué qu'elle avait reçu de nombreuses plaintes récemment concernant une escroquerie par message texte portant sur la Prestation canadienne d'urgence (PCU), l'une des nombreuses aides financières offertes par le gouvernement fédéral en réponse à la pandémie.¹ Selon la police, un message texte comprenant un lien ou une pièce jointe avise que la PCU a été déposée au compte du destinataire. La police a mis en garde le public contre le risque de cliquer sur le lien ou la pièce jointe au message texte, ce qui entraînerait l'installation d'un logiciel malveillant sur le téléphone, ou l'ouverture d'un site Web où on demande à la victime de fournir des renseignements personnels. L'une ou l'autre de ces options peut conduire à une usurpation d'identité. Si vous recevez ce message texte, la police vous déconseille de cliquer sur les liens ou les pièces qu'il contient.

En outre, la GRC² fournit d'autres exemples de fraudes qui ont été commises durant la pandémie de la COVID-19 :

- Des sociétés privées proposent d'acheter un test de dépistage de la COVID-19 simple et rapide.
- Des vendeurs itinérants offrent de faux services de décontamination.
- Des fraudeurs se font passer pour des policiers et imposent des amendes ponctuelles à des citoyens portant des masques sous prétexte que le port d'un masque en public va à l'encontre de la *Loi sur le voile intégral*.
- Des investisseurs subissent des pressions pour investir dans de nouvelles actions liées au virus.
- Des publicités frauduleuses, par courriel, message texte ou annonces-éclair en ligne qui exploitent les craintes du public se rapportant à la COVID-19;

- Des publicités frauduleuses en ligne proposent des produits de nettoyage, des désinfectants pour les mains et d'autres articles qui sont très en demande.

Malheureusement, la fraude n'est pas un phénomène nouveau au Canada; les fraudeurs tentent incessamment, depuis des années, de faire fortune en usant de moyens illégaux, aux dépens d'autres personnes. Ils se font souvent passer pour des représentants de l'Agence du revenu du Canada (ARC) pour tromper leurs victimes. En voici un exemple, fourni par l'ARC :

Récemment diplômée, Anne est une jeune professionnelle qui débute sa carrière. Un jour, alors qu'elle est au travail, elle reçoit un appel d'un numéro qu'elle ne reconnaît pas. La personne au téléphone s'identifie comme un employé de l'ARC et informe Anne qu'elle appelle au sujet de sa dette impayée afin de confirmer ses renseignements personnels, notamment sa date de naissance et le numéro de son compte bancaire, et de mettre sur pied un plan de retraits systématiques afin de rembourser la dette.

Anne ne se souvient pas qu'elle doit de l'argent à l'ARC. De plus, elle ne se souvient pas d'avoir fourni à l'ARC son numéro de téléphone au bureau. Lorsqu'elle exprime ces préoccupations, son interlocuteur s'énerve et prévient Anne qu'elle risque des poursuites si elle ne coopère pas. Bien qu'elle ressente une certaine appréhension, elle n'a jamais eu affaire avec l'ARC et suppose que la demande doit être bien fondée. Elle accepte à contrecœur de fournir les renseignements demandés.

De nombreux Canadiens, notamment des personnes âgées, ont été victimes d'hameçonnage par téléphone. Les personnes qui ne sont pas au courant de ce genre de fraude sont facilement manipulées par les fraudeurs qui volent leur identité ou leur argent. Les contribuables doivent donc être vigilants lorsqu'ils reçoivent un appel, un courriel, de la correspondance par la poste ou un message texte qui semblent provenir de l'ARC, surtout s'ils ont pour but d'obtenir des renseignements personnels, tels qu'un numéro d'assurance sociale, de carte de crédit, de compte bancaire ou de passeport, et que le ton des communications est intimidant, voire contraignant ou menaçant, afin de soustraire de l'argent des victimes.

¹ Rendez-vous sur la page Web <https://www.canada.ca/fr/ministere-finances/plan-intervention-economique.html> pour prendre connaissance du Plan d'intervention économique du Canada pour répondre à la COVID-19. ² Gendarmerie royale du Canada.

Comment pouvez-vous savoir si vous êtes vraiment contactés par l'ARC?

Pour éviter d'être victime de ce type de fraude, les contribuables doivent pouvoir déterminer s'ils sont vraiment contactés par l'ARC.

Par téléphone³	
<i>Raisons valides de vous contacter par téléphone :</i>	<i>L'ARC ne vous contactera jamais par téléphone pour les raisons suivantes :</i>
<ul style="list-style-type: none">• Vérification de l'identité d'une personne en lui demandant de fournir des renseignements personnels, tels que son nom, sa date de naissance, son adresse ou son numéro d'assurance sociale;• Demande de renseignements sur un compte dans le cadre d'une enquête au sujet d'une entreprise;• Demande de renseignements dans le cadre d'une vérification;• Offre de conseils fiscaux à une petite entreprise.	<ul style="list-style-type: none">• Demande de renseignements relatifs à un passeport, une carte de santé ou un permis de conduire;• Demande de paiement immédiat, soit par virement électronique, bitcoin, carte de crédit prépayée ou carte-cadeau;• Profération de menaces d'arrestation ou d'emprisonnement;• Tentative d'obtenir des renseignements personnels en invitant les victimes à remplir un formulaire en ligne en cliquant sur un lien dans un courriel.

Par courriel³	
<i>Raisons valides de vous contacter par courriel :</i>	<i>L'ARC ne vous contactera jamais par courriel pour les raisons suivantes :</i>
<ul style="list-style-type: none">• Envoi d'un avis par courriel lorsqu'un nouveau message ou un document, tel qu'un avis de cotisation, est disponible pour être consulté sur les portails sécurisés de l'ARC;• Envoi d'un courriel contenant un lien vers une page Web, un formulaire ou une publication de l'ARC suite à la demande d'un contribuable faite par téléphone ou lors d'une rencontre avec un agent.	<ul style="list-style-type: none">• Donner ou demander des renseignements personnels ou financiers par courriel et demander aux contribuables de cliquer sur un lien;• Envoi par courriel d'un lien demandant de remplir un formulaire en ligne et de fournir des renseignements personnels ou financiers;• Envoi d'un courriel comportant un lien sur lequel le contribuable doit cliquer pour obtenir un remboursement;• Demande de paiement immédiat par virement électronique, bitcoin, cartes de crédit prépayées ou cartes-cadeaux;• Profération de menaces d'arrestation ou d'emprisonnement.

Par la poste³	
<i>Raisons valides de vous envoyer du courrier :</i>	<i>L'ARC ne vous enverra jamais de courrier pour les raisons suivantes :</i>
<ul style="list-style-type: none">• Demande de renseignements financiers, tels que le nom et l'adresse de votre banque;• Envoi d'un avis de cotisation ou de nouvelle cotisation;• Demande de paiement d'un montant dû par le biais de l'une des options de paiement de l'ARC;• Avis relatif au recouvrement d'une dette impayée;• Demande de renseignements par écrit dans le cadre d'une vérification;• Offre de conseils fiscaux à une petite entreprise.	<ul style="list-style-type: none">• Organiser une réunion dans un lieu public pour effectuer un paiement;• Demande de paiement immédiat par virement électronique, bitcoin, cartes de crédit prépayées ou cartes-cadeaux;• Profération de menaces d'arrestation ou d'emprisonnement.

Par message texte ou message instantané³
L'ARC ne communique jamais par message texte ou message instantané avec les contribuables. Si un contribuable reçoit des messages textes ou des messages instantanés prétendant provenir de l'ARC, il s'agit d'une escroquerie!

³Source : Agence du revenu du Canada (ARC).

Protégez-vous contre les fraudeurs

Quel que soit le type de fraude, le Centre antifraude du Canada a fourni les conseils suivants pour aider les Canadiens à se protéger contre la fraude :

N'hésitez pas à dire non : Ne vous laissez pas intimider par des tactiques de vente agressives et faites attention aux appels pressants qui jouent sur vos émotions.

Renseignez-vous : Vérifiez que la société avec laquelle vous faites affaires est légitime avant d'agir. Faites attention aux publicités mensongères ou trompeuses ou aux courriels frauduleux.

Ne fournissez pas d'informations personnelles : Méfiez-vous des appels non sollicités, surtout si votre interlocuteur vous demande des informations personnelles. Si vous n'avez pas effectué l'appel, vous ne savez pas à qui vous parlez.

Méfiez-vous des frais initiaux : Lors de nombreuses escroqueries, la victime est appelée à payer des frais avant de recevoir des produits, des services ou un prix. Sachez qu'il n'y a pas de frais ni d'impôt sur les prix au Canada – si vous remportez un prix, il devrait être gratuit.

Protégez votre ordinateur : Faites attention aux messages urgents qui s'affichent lorsque vous êtes en ligne. Ne cliquez pas sur ces messages et n'appellez pas le numéro fourni. Assurez-vous d'avoir installé un logiciel anti-virus et assurez-vous que votre système d'exploitation est à jour.

Que faire si vous êtes victime d'une escroquerie?

Si vous avez perdu de l'argent ou des objets de valeur, ou vous avez fourni des informations personnelles, contactez la police locale. Signalez également l'escroquerie au Centre antifraude du Canada (<https://antifraudcentre-centreantifraude.ca/report-signalez-fra.htm>).

AVIS IMPORTANTS

La présente communication est publiée par CI Investments Inc. (« CI »). Tout commentaire et toute information contenus dans cette communication sont fournis à titre de source générale d'information et ne doivent pas être considérés comme des conseils personnels de placement. Les données et les renseignements fournis par CI et d'autres sources sont jugés fiables à la date de publication.

Certains énoncés contenus dans la présente sont fondés entièrement ou en partie sur de l'information fournie par des tiers; CI a pris des mesures raisonnables afin de s'assurer qu'ils sont exacts. Les conditions du marché pourraient varier et donc influencer sur les renseignements contenus dans le présent document.

L'information contenue dans ce document ne constitue pas des conseils juridiques, comptables, fiscaux ou de placement et ne devrait pas être considérée comme telle. Il convient de consulter des conseillers professionnels avant d'agir en vertu des renseignements contenus dans cette publication.

Le contenu de cette communication ne peut, en aucune manière, être modifié, copié, reproduit, publié, téléchargé, affiché, transmis, distribué ou exploité commercialement. Le téléchargement, la retransmission, le stockage sur quelque support que ce soit, la reproduction, la redistribution ou la nouvelle publication à n'importe quelle fin sont strictement interdits sans la permission écrite de CI.

Placements CI® et le logo Placements CI sont des marques déposées de CI Investments Inc. « Partenaire de confiance en matière de patrimoine^{MC} » est une marque de commerce de CI Investments Inc.

© CI Investments Inc. 2020. Tous droits réservés.

Date de publication : 28 mai 2020.



630, boul. René-Lévesque Ouest, bureau 2900, Montréal (Québec) H3B 1S6 | www.ci.com

Bureau de Montréal
514-875-0090
1-800-268-1602

Toronto
416-364-1145
1-800-268-9374

Calgary
403-205-4396
1-800-776-9027

Vancouver
604-681-3346
1-800-665-6994

Service à la clientèle
1-800-792-9355

20-05-0667_F (05/20)