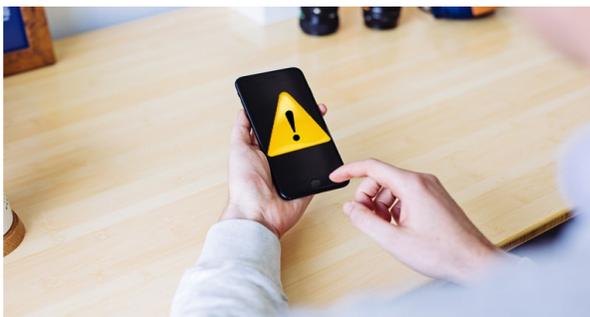


FAIRE FACE AUX FRAUDEURS

La fraude a toujours été présente dans notre société. Avec l'avènement des technologies, les fraudeurs possèdent de meilleurs moyens pour arnaquer dans l'anonymat. Le contexte de la pandémie ne freine pas les ardeurs de ces arnaqueurs, bien au contraire.

À la fin de l'automne 2020, bon nombre de Québécois ont appris de l'Agence du revenu du Canada (ARC) qu'ils avaient été victimes de fraude. En effet, le vol d'identité pour obtenir la Prestation canadienne d'urgence (PCU) aura été très lucratif pour les gens mal intentionnés. Par contre, pour moi, comme pour bien d'autres victimes, cela a été le début d'une longue série d'actions à poser pour comprendre et corriger la situation.

J'ai d'abord reçu une lettre de l'ARC m'indiquant que j'avais modifié mes coordonnées bancaires et que si cela n'était pas le cas, j'avais possiblement été victime d'une fraude. La lettre me donnait un numéro de téléphone à appeler pour clarifier la situation. En consommatrice avertie, j'ai d'abord vérifié sur internet que le numéro de téléphone inscrit correspondait bien à un numéro permettant de rejoindre l'ARC. Les fraudeurs ayant recours à des logiciels ou applications pour tromper leurs victimes, je savais que je devais vérifier les informations avant d'agir et de fournir toute information personnelle pour m'identifier.



Informations personnelles sensibles à protéger !

- Vos prénom et nom
- Vos adresses postale et électronique
- Votre date de naissance
- Votre numéro d'assurance sociale
- Vos numéros de permis de conduire et de passeport
- Vos données bancaires et de cartes de crédit
- Votre signature

J'ai par la suite tenté de rejoindre l'ARC par téléphone. Après quelques tentatives et trois heures d'attente au téléphone, la ligne a coupé et tout aurait été à recommencer. J'ai donc rejoint le bureau de mon député fédéral pour avoir de l'aide. Avec mon autorisation, son personnel a pu me confirmer que j'avais été victime d'une fraude et qu'une personne avait demandé la PCU en mon nom. Pour corriger la situation et éviter d'avoir à inclure les sommes de PCU dans mes revenus annuels, plusieurs démarches devaient être complétées.



On m'a informée que je devais contacter le service de police local afin de faire une déposition. L'obtention d'un numéro de dossier me permettait alors de confirmer que j'avais été victime d'une fraude et que ce n'était pas moi qui avais reçu la PCU. Je devais ensuite faire parvenir ce numéro de dossier à l'ARC. J'ai aussi rapidement communiqué avec mon institution financière ainsi qu'avec les bureaux de crédit Équifax et TransUnion pour les informer que j'avais été victime de fraude. Dans mon cas, mon institution a même pu m'offrir du support pour les démarches à faire.

On m'a également conseillé de communiquer avec le Centre antifraude du Canada, ce que j'ai fait. Sur leur site, j'ai trouvé de nombreux trucs pour me protéger et améliorer ma vigilance. <https://antifraudcentre-centreantifraude.ca/index-fra.htm>

Les démarches faites m'ont permis d'alerter toutes les institutions et organismes pertinents, ce qui va freiner les fraudeurs s'ils tentent à nouveau d'utiliser mes données.

Cette expérience m'a aussi permis d'aider une connaissance qui a reçu à tort un relevé fiscal pour la PCU alors qu'elle ne l'avait jamais demandée ni reçue. Je lui ai suggéré de faire les mêmes démarches que moi, ce qui lui permettra de corriger sa situation et d'en limiter les répercussions.

L'hameçonnage est un stratagème très répandu pour soutirer des renseignements personnels à une victime. Par exemple, le fraudeur envoie un texto ou un courriel au nom du gouvernement. Un lien est inclus dans le message vers un formulaire en ligne dans lequel il faut entrer des informations personnelles pour recevoir un remboursement. Il ne faut pas cliquer sur le lien! Le même procédé peut s'effectuer via le téléphone. Il ne faut pas supposer que le numéro sur l'afficheur est exact. Il ne faut pas tomber dans ce piège! Les gouvernements ne communiquent pas avec les citoyens par courriel ou téléphone et connaissent déjà leurs données personnelles. On doit se méfier de toute communication qui presse à agir ou fait miroiter quelque chose de trop beau pour être vrai.

Vous êtes victime de fraude, de vol ou d'extorsion?

- Avisez le gouvernement ou l'entreprise concernés.
- Faites une déposition au service local de police.
- Communiquez avec votre institution financière.
- Contactez les bureaux de crédit Équifax et TransUnion.
- Informez le Centre antifraude du Canada.

