Le Centre antifraude du Canada (CAFC) souhaite sensibiliser la population canadienne à l'importance de protéger ses renseignements personnels et financiers. Les fraudeurs recueillent des renseignements de différentes façons, en se servant notamment des médias sociaux, du courrier électronique, de SMS, de formulaires et sondages en ligne, ainsi que de l'information accessible au public et de données piratées. Des détails comme le nom, la date de naissance, le numéro de téléphone, l'employeur, l'entourage familial, les projets de voyage ou les activités sur les médias sociaux peuvent sembler anodins. Pourtant, mis bout à bout, ils permettent aux fraudeurs de se faire une idée plus précise d'une personne.

Les fraudeurs utilisent ces renseignements à plusieurs fins : créer un scénario convaincant, se faire passer pour la personne ou une de ses connaissances, ou rendre une prise de contact plus vraisemblable. Les renseignements sensibles, comme ceux qui figurent sur les pièces d'identité délivrées par le gouvernement, les numéros d'assurance sociale (NAS), les renseignements bancaires et de cartes de crédit, leur servent à commettre des fraudes par usurpation d'identité et d'autres crimes financiers. Par ailleurs, les renseignements recueillis aujourd'hui peuvent être conservés afin d'être associés à d'autres obtenus ultérieurement. Les fraudeurs n'ont pas toujours besoin de renseignements sensibles. Souvent, la combinaison de plusieurs éléments d'information d'apparence anodine leur est tout aussi utile.

Signaux d'alerte

Soyez prudent si :

- on vous demande soudainement de fournir ou de confirmer des renseignements personnels ou financiers;
- on vous demande sans raison valable de fournir la copie ou la photo d'une pièce d'identité délivrée par le gouvernement;
- vous recevez de manière impromptue un courriel, un SMS ou un message dans les médias sociaux vous dirigeant vers un site Web ou un formulaire destiné à recueillir vos renseignements personnels;
- une personne utilise des renseignements sur vous, votre lieu de travail ou votre famille pour vous mettre en confiance ou dérouler un récit plus convaincant;
- on vous demande avec insistance de fournir sur-le-champ des renseignements personnels ou financiers;
- vous recevez des factures, des relevés ou de la correspondance au sujet de comptes ou de services que vous n'avez pas souscrits;
- Vous remarquez des opérations, des demandes de crédit ou d'autres activités que vous n'avez pas autorisées.

Comment vous protéger

- Mieux vaut prévenir que guérir. Réfléchissez à deux fois à l'information que vous vous apprêtez à rendre publique et aux personnes qui peuvent la consulter.
- Passez en revue les paramètres de confidentialité de vos comptes de médias sociaux et limitez les renseignements personnels accessibles au public.
- Soyez prudent lorsque vous partagez votre date de naissance, vos projets de voyage, votre lieu de travail, de l'information sur votre famille et d'autres détails personnels en ligne.
- Protégez vos renseignements sensibles, notamment votre NAS, vos renseignements bancaires et de carte de crédit et vos pièces d'identité délivrées par le gouvernement.
- Avant de fournir des renseignements personnels, posez-vous la question de savoir qui les demande, pourquoi ils sont nécessaires et si vous vous attendiez à ce qu'on vous les demande.
- Ne fournissez pas de renseignements personnels ou financiers à une personne qui communique avec vous par téléphone, courriel, SMS ou sur les médias sociaux de façon impromptue.
- Vérifiez par vous-même la légitimité des demandes de renseignements que vous recevez en utilisant des coordonnées sourcées, c'est-à-dire officielles.
- Évitez de cliquer sur des liens ou de remplir des formulaires en ligne destinés à recueillir vos renseignements personnels lorsque vous n'êtes pas à l'origine de la démarche.
- Soyez prudent avec les sondages, les concours et les promotions qui vous demandent plus de renseignements personnels que nécessaire.
- Examinez régulièrement vos relevés et votre dossier de crédit pour détecter toute activité suspecte.

Quiconque croit avoir été la cible de fraude ou de cybercriminalité est prié de le signaler à son service de police local, puis de faire un signalement en ligne sur le site Web Signaler la cybercriminalité et la fraude ou par téléphone au 1-888-495-8501.