Se protéger de la fraude

2020

Au Canada comme ailleurs, les fraudeurs sont créatifs lorsqu'il est question d'extorquer de l'argent. Le risque d'escroquerie par téléphone, par courriel, par message texte ou en personne est réel. Alors qu'il existe des recours pour les victimes de fraude, les conséquences peuvent toutefois être importantes et il est essentiel d'être vigilant.

Mesures générales de protection

Ne jamais partager votre numéro d'identification personnel (NIP) avec qui que ce soit;

Utiliser un mot de passe sûr et différent pour chacun de vos comptes en ligne;

Vérifier vos relevés de compte et investiguer sur toute transaction qui semble irrégulière;

Lors d'investissements, vous assurer de faire affaire avec un professionnel et vous méfier des offres qui semblent trop alléchantes, des occasions qui demandent de prendre une décision immédiatement et des promesses de rendement élevé sans risque en retour (même si elles viennent d'une personne que vous connaissez).

Lorsque vous croyez être victime de fraude, il faut rapporter immédiatement la situation aux autorités. Il faut également faire annuler toute carte que vous croyez compromise et changer le mot de passe des comptes que vous croyez à risque.

Achats en ligne

Il faut faire preuve de prudence lorsqu'on achète quelque chose en ligne :

- Utiliser un moyen de paiement sécurisé (comme un virement Interac ou PayPal) lors de transactions entre particuliers;
- Dans le cas d'une transaction avec un commerçant, il faut vous assurer qu'il existe réellement;
- Vérifier que le site utilisé est sécuritaire, que l'adresse du site Web commence par « https » (le « s » signifie « sécurisé ») et que l'image d'un cadenas fermé apparaît à sa gauche dans la barre d'adresse du navigateur.

Appels téléphoniques et courriels suspects

Il faut également vous méfier des appels téléphoniques ou des courriels que vous recevez de la part de votre institution financière, de l'Agence du revenu du Canada ou de toute autre organisation similaire, surtout si :

- On vous demande des informations personnelles pour confirmer votre identité (ex. : mot de passe, numéro d'assurance sociale, date de naissance, numéro de compte ou de carte de crédit, etc.);
- On insiste pour que vous payiez un montant d'argent immédiatement;
- On vous promet un remboursement ou tout autre montant intéressant;
- On vous demande de cliquer sur un lien ou de vous connecter à votre compte en ligne;
- On utilise des menaces de répercussions financières, judiciaires ou autres.

En cas de doute, il faut mettre fin à l'échange et appeler vous-même l'organisation en utilisant votre numéro officiel.

Canada | AFY

Pour plus d'information, voir la section « Escroqueries et fraudes » du site Web de la Gendarmerie royale du Canada et la rubrique « Protection contre la fraude et les escroqueries » de la section « Argent et finances » sur le site du gouvernement du Canada.