CANADIAN ANTI-FRAUD CENTRE BULLETIN

Enquêteur bancaire 2025-06-27

FRAUD: RECOGNIZE, REJECT, REPORT

Le Centre antifraude du Canada souhaite mettre en garde la population canadienne contre une augmentation des signalements liés à des fraudes de l'enquêteur bancaire. Les fraudeurs se font passer pour des institutions financières, des forces de l'ordre, Amazon ou des agences d'évaluation du crédit et prétendent que le compte bancaire de la victime a été compromis.

Dans certains cas, les fraudeurs fournissent certains renseignements personnels sur la victime, comme son nom, sa date de naissance, son numéro de téléphone, son adresse, son numéro d'assurance sociale et son numéro de carte de débit, afin de donner l'impression que l'appel est légitime. Les fraudeurs falsifient également les numéros de téléphone d'institutions financières, de forces de l'ordre et d'agences d'évaluation du crédit ou fournissent des numéros de téléphone de rappel frauduleux qui semblent correspondre à ceux d'institutions financières.

<u>Variantes de la fraude de l'enquêteur bancaire :</u>

1.) Les victimes reçoivent un appel téléphonique automatisé prétendument de leur institution financière, de forces de l'ordre, d'une agence d'évaluation du crédit (Equifax® Canada ou Transunion) ou, dans certains cas, d'Amazon, les informant qu'il y a eu des transactions frauduleuses dans leur compte. Les fraudeurs demandent aux victimes l'accès à leur ordinateur ou à leur appareil, afin de poursuivre « l'enquête ». Ils montrent alors aux victimes une transaction frauduleuse dans leur compte bancaire en ligne. Les fraudeurs disent qu'ils veulent l'aide des victimes dans le cadre d'une « enquête » visant des criminels qui leur auraient volé de l'argent; les fraudeurs demandent donc aux victimes de leur envoyer de l'argent dans le cadre de cette enquête.

   Dans certains cas, les fraudeurs ajoutent les victimes à la liste des « bénéficiaires » à l'aide d'une adresse électronique frauduleuse et les informent qu'elles doivent transférer une grosse somme d'argent pour protéger leur compte. Les fraudeurs convainquent les victimes qu'ils ont versé de l'argent dans leur compte, alors qu'en réalité, les fonds ont été transférés de leur ligne de crédit ou de leur compte d'épargne.

2.) Il se peut que les fraudeurs aient le numéro de carte de débit et le mot de passe des victimes, mais qu'ils n'aient pas accès au compte de celles-ci en raison de l'authentification multifacteur. Les fraudeurs contactent ensuite les victimes en prétendant être leur institution financière et les

informent qu'elles doivent fournir un code qu'elles recevront par SMS ou par courrier électronique afin de confirmer leur identité. Le code fourni par les victimes est le code d'authentification multifacteur qui donne aux fraudeurs un accès complet au compte bancaire de celles-ci.

3.) Les fraudeurs informeront les victimes qu'aux fins de l'enquête, ils doivent récupérer la carte de débit ou de crédit des victimes à leur domicile. Ils se rendent donc au domicile des victimes pour récupérer la carte et, pour rendre leur intervention encore plus crédible, ils peuvent même leur demander de couper la carte en deux, mais sans endommager la puce. Si les victimes ne coopèrent pas, ils peuvent même aller jusqu'à les menacer de les arrêter.

Indices – Comment se protéger

- Les fraudeurs utilisent la technique de falsification des données de l'appelant pour induire les victimes en erreur. Il ne faut pas présumer que les numéros de téléphone qui apparaissent sur votre afficheur sont authentiques.
- Si vous recevez un appel d'un supposé employé de votre institution financière, dites-lui que vous le rappellerez. Mettez fin à l'appel et composez le numéro inscrit au dos de votre carte de débit à partir d'un autre téléphone ou attendez une dizaine de minutes avant de faire l'appel.
- Les agences d'évaluation du crédit ne vous appelleront pas au hasard, sauf s'il s'agit d'une demande de rappel. Si vous recevez un appel d'un supposé employé d'une telle agence, dites-lui que vous le rappellerez. Visitez le site web de l'agence et composez le numéro de téléphone officiel qui y est indiqué.
- Ces institutions ou les forces de l'ordre ne vous menaceront jamais au téléphone.
- Ne communiquez à personne les codes reçus par SMS ou par courrier électronique. Dans la plupart des cas, il s'agit de codes d'authentification multifacteur qui permettent aux fraudeurs d'accéder à votre compte.
- Les fraudeurs fournissent souvent les quatre à six premiers numéros de votre carte de débit ou de crédit. En fait, ces numéros permettent simplement d'identifier l'émetteur de la carte; il s'agit du numéro d'identification bancaire. La plupart des numéros de cartes de débit et de crédit émises par une même institution financière commencent par les mêmes quatre à six chiffres.
- Si vos renseignements personnels ont déjà été compromis dans le cadre d'une intrusion ou d'un courriel hameçon, n'oubliez pas qu'ils peuvent servir à donner à la communication une apparence légitime.
- Ne donnez jamais accès à votre ordinateur à distance.
- Les représentants d'institutions financières et de commerces en ligne ne demandent jamais de transférer des fonds dans un compte externe pour des raisons de sécurité.
- Les institutions financières et les services de police ne demandent **jamais** de remettre une carte bancaire et ne vont pas chercher des cartes au domicile des particuliers.
- Pour une protection supplémentaire, vous pouvez activer la fonction de dépôt automatique de fonds reçus par virement électronique.
- Obtenez d'autres conseils et astuces pour vous protéger contre la fraude.

Si vous pensez avoir été victime d'une fraude, signalez-la à votre service de police local et au système de signalement en ligne du Centre antifraude du Canada ou par téléphone, au 1-888-495-8501. Que vous soyez la victime ou non, vous devriez tout de même signaler l'incident au Centre antifraude du Canada.