BULLETIN DU CENTRE ANTIFRAUDE DU CANADA

Nouvelle variante du stratagème du faux enquêteur bancaire 2024-08-23

LA FRAUDE : IDENTIFIEZ-LA, SIGNALEZ-LA, ENRAYEZ-LA

Le Centre antifraude du Canada (CAFC) tient à avertir la population canadienne qu'il existe une nouvelle variante du stratagème du faux enquêteur bancaire. Des fraudeurs se font passer pour des employés d'institutions bancaires, et prétendent que le compte bancaire de la victime a été compromis.

Les fraudeurs convainquent les victimes que pour protéger leur compte jusqu'à ce qu'une nouvelle carte de débit soit émise, elles doivent envoyer une transaction de virement Interac à leur propre numéro de téléphone portable. Le suspect indiquera à la victime les étapes à suivre pour s'ajouter en tant que bénéficiaire et pour augmenter sa limite quotidienne de virement Interac à 10 000 $ (il est à noter que le montant maximal qu'un expéditeur peut envoyer par l'intermédiaire du réseau de virement Interac peut varier selon l'institution financière de l'expéditeur). Interac refusera automatiquement d'effectuer tout paiement d'un expéditeur dépassant la limite fixée par l'établissement financier. Le suspect fournit la question et la réponse du virement électronique que la victime doit utiliser pour le virement. Une fois que la victime a envoyé la transaction de virement électronique Interac à son propre numéro de téléphone portable, les suspects lui demandent un « code » qui est la dernière partie de l'URL/du lien de virement électronique Interac reçu. Si la victime fournit l'URL, les suspects pourront déposer les fonds sur leur propre compte.

Dans certains cas, les suspects peuvent fournir certains renseignements personnels de la victime, dont son nom, sa date de naissance, son numéro de téléphone, son adresse et son numéro de carte de débit pour que l'appel semble légitime. D'après les fraudes signalées au CAFC, les suspects falsifient les numéros de téléphone d'institutions financières, ou fournissent des numéros de téléphone de rappel frauduleux qui semblent correspondre à l'institution financière.

<u>Autres variantes du stratagème du faux enquêteur bancaire :</u>

1.) La victime reçoit un appel automatisé provenant soi-disant de leur institution financière, d'un organisme d'application de la loi ou, dans certains cas, d'Amazon qui l'avise de transactions frauduleuses survenues sur son compte. Les fraudeurs demandent aux victimes d'avoir accès à leur ordinateur pour poursuivre l'« enquête ». Ils leur montrent ensuite une transaction frauduleuse dans leur compte bancaire en ligne. Les suspects demandent aux victimes de les aider à enquêter sur les criminels qui ont volé leur argent, et d'envoyer des fonds dans le cadre de cette enquête.

   Parfois, les fraudeurs ajoutent la victime comme « bénéficiaire » avec une adresse de courriel frauduleuse, et demandent à la victime de virer une grosse somme d'argent pour protéger leur compte. Les fraudeurs convainquent la victime qu'ils ont ajouté des fonds au compte de la victime, mais en réalité, les fonds ont été transférés depuis leur marge de crédit ou leur compte d'épargne.

2.) Les suspects pourraient avoir le numéro de carte de débit de la victime et son mot de passe, mais ne peuvent pas accéder au compte de la victime à cause de l'authentification multifacteur qui protège leur compte. Les suspects communiquent alors avec la victime en prétendant être des employés de leur institution financière, et demandent à la victime de leur fournir le code reçu dans un texto ou un courriel pour confirmer son identité. Le code fourni par la victime est le code d'authentification multifacteur, qui donne aux suspects l'accès complet à son compte bancaire.

Indices – Comment vous protéger

- Les fraudeurs utilisent la technique de « falsification des données de l'appelant » pour induire les victimes en erreur. Ne présumez pas 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 ou de crédit à partir d'un autre téléphone ou attendez une dizaine de minutes avant de faire l'appel.
- Ne fournissez jamais aux fraudeurs des détails sur les liens ou adresses URL reçus par texto ou par courriel.
- Ne divulguez à personne les codes reçus par texto ou par courriel. Dans la plupart des cas, ce sont des codes d'authentification multifacteur qui donneront aux fraudeurs accès à votre compte.
- Les fraudeurs vous fourniront souvent les quatre à six premiers chiffres de votre carte de débit ou de crédit. N'oubliez pas que la plupart des numéros de carte de débit ou de crédit d'une même institution financière commencent par les mêmes quatre ou six chiffres.
- Si vos renseignements personnels ont été compromis par le passé dans le cadre d'une intrusion ou d'un courriel hameçon, n'oubliez pas que ces renseignements 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.
- Obtenez d'autres conseils pour vous protéger contre la fraude.

Si vous croyez avoir été la cible d'un acte de cybercriminalité ou de fraude, vous devez le signaler à votre service de police local et au CAFC au moyen de son système de signalement en ligne ou par téléphone au 1-888-495-8501. Il est recommandé de signaler une fraude, que vous en ayez été victime ou non, au CAFC.