BULLETIN DU CENTRE ANTIFRAUDE DU CANADA

Fraudeurs se faisant passer pour le CAFC 05-06-2025

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

Le Centre antifraude du Canada (CAFC) met en garde le public contre les fraudeurs qui se font passer pour le CAFC. Les fraudeurs utilisent les noms des employés du CAFC, falsifient le numéro de téléphone du CAFC et les adresses courriel. Ils envoient de faux messages promettant de l'aide pour des enquêtes et/ou le remboursement de fonds perdus.

Voici des exemples courants d'arnaques où les fraudeurs prétendent représenter le CAFC :

Enquêteur bancaire :
Les victimes sont contactées par quelqu'un prétendant provenir de leur institution financière, d'Amazon ou des forces de l'ordre, y compris le CAFC. Le fraudeur affirme qu'il y a une activité suspecte sur le compte bancaire ou la carte de crédit de la victime et qu'il veut l'aider à récupérer l'argent ou à sécuriser le compte.

Arnaques de soutien technique :
Les victimes peuvent recevoir des appels non sollicités ou des messages contextuels prétendant qu'il y a un problème avec leur ordinateur ou appareil. Les fraudeurs peuvent alors convaincre la victime d'accorder l'accès à distance à l'appareil ou de payer pour un « service nécessaire ».

Dans certains cas, les fraudeurs prétendent être du CAFC et disent aux victimes que si elles ne coopèrent pas avec eux, elles risquent d'être arrêtées en raison d'une fraude commise à leur nom.

Fraudes de récupération :
Les fraudeurs se font passer pour le CAFC ou les forces de l'ordre pour établir la confiance et convaincre les victimes. Ils prétendent aider à récupérer de l'argent perdu et demandent un paiement pour récupérer les fonds. Les fraudeurs peuvent également envoyer de faux documents, des profils de médias sociaux ou d'autres éléments pour paraître légitimes.

Le CAFC ne demandera **JAMAIS** :

- D'informations personnelles comme votre NAS, vos informations bancaires ou votre permis de conduire
- Un paiement sous aucune circonstance
- Un mot de passe ou un code d'authentification (p. ex. code MFA)
- Un virement d'argent pour la récupération de fonds
- D'accéder à distance à votre appareil
- De payer à l'avance pour obtenir un remboursement
- Vos identifiants de connexion
- De l'aide dans des publicités sur les médias sociaux

Comment vous protéger :

- Si vous recevez un appel ou un courriel prétendant venir du CAFC, demandez le nom de l'appelant et contactez le CAFC directement en appelant le 1-888-495-8501 ou communiquez avec votre service de police local.
- Ne partagez pas de codes reçus par texto ou courriel avec des personnes inconnues, surtout si elles essaient d'accéder à vos comptes.
- Ne donnez jamais accès à distance à vos appareils.
- N'hésitez pas de raccrocher.
- Ne laissez jamais une personne inconnue accéder à distance à votre ordinateur/appareil.
- Faites toujours inspecter votre appareil par un professionnel local réputé.
- Ne payez jamais à l'avance pour un remboursement.
- Apprenez-en davantage sur les trucs et astuces pour vous protéger.

Toute personne qui croit être victime d'une cybercriminalité ou d'une fraude doit le signaler à la police et au CAFC en ligne ou par téléphone au 1-888-495-8501.