CANADIAN ANTI-FRAUD CENTRE BULLETIN

20 ans de fraude – Méthodes de sollicitation 2024-03-11

FRAUD: RECOGNIZE, REJECT, REPORT

L'année 2024 marque le 20e anniversaire du Mois de la prévention de la fraude. Le thème de cette année est : **« 20 ans de lutte contre la fraude : d'hier à aujourd'hui »**. Ce thème nous amènera à nous pencher sur l'évolution de certaines fraudes à l'ère numérique et à établir des comparaisons utiles entre le passé et le présent.

Le présent bulletin met en lumière certaines des principales méthodes de sollicitation utilisées selon les signalements transmis au Centre antifraude du Canada (CAFC). La plupart des méthodes de sollicitation utilisées actuellement par les fraudeurs existaient déjà il y a 20 ans, mais la façon dont elles sont employées a évolué.

Voici les principales méthodes de sollicitation utilisées par les fraudeurs pour entrer en contact avec leurs victimes :

Téléphone

Selon les signalements effectués en 2023, le téléphone était la principale méthode de sollicitation utilisée par les fraudeurs. Ces 20 dernières années, la technologie entourant les appels frauduleux a évolué. Les fraudeurs sont maintenant en mesure de falsifier les numéros de téléphone d'où proviennent les appels et de faire des appels automatisés. À cause de l'évolution de la technologie, les fraudeurs peuvent cibler beaucoup plus de Canadiens depuis quelques années. Les fraudeurs prétendent souvent être des proches de la victime ou des représentants de la police, d'institutions financières ou du gouvernement.

Cyberfraude (courriel, Internet, médias sociaux et messagerie texte)

En 2023, plus de 75 % des pertes signalées étaient attribuables à la cyberfraude. Par conséquent, le CAFC insiste sur l'évolution du monde virtuel ces 20 dernières années et sur l'incidence de ces changements sur la fraude.

Les plateformes de médias sociaux sont devenues l'un des principaux outils que les fraudeurs utilisent pour cibler leurs victimes. Les fraudeurs exploitent les médias sociaux pour cibler les Canadiens en utilisant des annonces frauduleuses, des comptes de médias sociaux compromis ou des robots pour recueillir des données personnelles.

La fraude par courrier électronique existait il y a 20 ans, mais de nos jours, les fraudeurs utilisent la technologie pour rendre leurs courriels frauduleux plus crédibles. La fraude par courrier électronique est plus complexe depuis que les fraudeurs falsifient l'adresse courriel de l'expéditeur pour hameçonner les victimes et infiltrent les réseaux avant une attaque d'hameçonnage.

Poste

La fraude par la poste a beaucoup diminué ces 20 dernières années, mais le CAFC continue de recevoir des signalements de cette nature. Les lettres frauduleuses peuvent par exemple être de fausses lettres d'héritage annonçant que vous avez droit à une importante somme d'argent parce qu'un parent éloigné est décédé. Les fraudeurs envoient aussi des lettres frauduleuses annonçant que le destinataire a gagné le gros lot. Si vous appelez au numéro donné, on vous demandera de payer certains frais ou une assurance.

Porte-à-porte ou en personne

La fraude en personne n'a pas beaucoup changé depuis 20 ans. Les fraudeurs peuvent offrir un service de peu de valeur ou vous demander de signer un contrat afin d'obtenir de l'équipement qui ne fonctionne pas bien. Des entrepreneurs malhonnêtes peuvent offrir des services de rénovation (travaux de toiture, pavage d'entrée ou aménagement paysager) à un faible coût. Les fraudeurs qui font du porte-à-porte utilisent fréquemment des tactiques de vente sous pression. Après avoir reçu le paiement, un dépôt ou un acompte, ils disparaissent ou offrent un service de piètre qualité.

Indices – Comment vous protéger

- Les fraudeurs utilisent la technique de falsification des données de l'appelant pour induire les victimes en erreur. Ne présumez jamais que les numéros de téléphone qui apparaissent sur votre afficheur sont authentiques.
- Si vous recevez un message suspect ou étrange de la part d'un ami en qui vous avez confiance, communiquez avec cette personne par un autre moyen afin de confirmer qu'elle vous a bel et bien envoyé le message.
- Si vous recevez un courriel ou un message texte non sollicité dans lequel on vous demande de cliquer sur un lien ou d'ouvrir une pièce jointe, ne le faites pas!
- Si vous recevez un message d'une entreprise, n'utilisez pas les coordonnées fournies dans le message. Cherchez les coordonnées officielles de l'entreprise et communiquez avec elle directement.
- Faites affaire avec des fournisseurs de services de bonne réputation établis dans votre région.
- Trouvez et vérifiez les coordonnées du fournisseur de service –adresse, numéro de téléphone, adresse de courriel—avant de payer pour obtenir un service.

- Méfiez-vous des lettres où un héritage vous est offert, souvent par de prétendus avocats ou comptables.
- Si vous recevez une lettre vous annonçant que vous avez gagné un prix, sachez que vous n'avez pas à payer de frais à l'avance pour recevoir votre prix.
- Prenez connaissance d'autres conseils et trucs pour vous protéger.

Si vous pensez avoir été victime de cybercriminalité ou de fraude, signalez-la à votre service de police local et au système de signalement en ligne du CAFC ou par téléphone au 1-888-495-8501. Si un incident s'est produit, mais que vous n'êtes pas tombé dans le piège, signalez-le tout de même au CAFC.