CANADIAN ANTI-FRAUD CENTRE
CENTRE ANTIFRAUDE DU CANADA

1re semaine du Mois de la cybersécurité : repérer la fraude dans un paysage numérique en mutation

2026-10-05

FRAUD: RECOGNIZE, REJECT, REPORT IT LA FRAUDE: IDENTIFIEZ-LA, SIGNALEZ-LA, ENRAYEZ-LA

Le Mois de la sensibilisation à la cybersécurité est l'occasion pour les Canadiens d'apprendre à reconnaître la fraude et les cybermenaces et à prendre des mesures simples pour se protéger. Le thème de cette année, « **La meilleure défense, c'est vous** », souligne le rôle important que chacun joue dans la protection de ses renseignements personnels, financiers et de ses comptes.

Les fraudeurs continuent d'adapter leurs modes opératoires aux nouvelles technologies, à l'actualité et à la façon dont les Canadiens communiquent. Ils communiquent avec leurs cibles par téléphone, SMS, courriel, médias sociaux ou par l'entremise d'un site Web. Ils se font passer pour un membre de la famille, une institution financière, un organisme gouvernemental, un corps policier, une entreprise ou une organisation connue et de confiance.

La fraude n'est pas toujours reconnaissable d'emblée. Un message peut être bien rédigé, un site Web peut avoir une apparence professionnelle et un numéro de téléphone peut sembler familier; autant d'éléments qui peuvent laisser croire qu'il s'agit d'une communication légitime, alors qu'ils ne prouvent pas que l'auteur est bien la personne qu'il prétend être.

L'ingénierie sociale pour influencer vos décisions

L'ingénierie sociale consiste pour le fraudeur à vous manipuler pour influencer vos décisions ou vous convaincre d'agir. Les fraudeurs exploitent souvent le sentiment d'urgence, la peur, l'autorité, l'excitation et la confiance pour vous amener à agir avant de réfléchir.

Ils prétendent que votre compte bancaire est compromis, que vous devez de l'argent, qu'un de vos proches a des problèmes ou que vous devez agir rapidement sous peine d'en subir les conséquences. Ils peuvent vous faire miroiter un prix, un investissement alléchant ou une occasion extraordinaire. D'autres tissent lentement leur toile afin de gagner votre confiance pour ensuite vous demander de l'argent ou des renseignements personnels.

Le scénario change, mais l'objectif reste le même : manipuler vos émotions et vous amener à agir les yeux fermés.

L'intelligence artificielle rend la fraude plus convaincante

L'intelligence artificielle (IA) rend le contenu frauduleux encore plus vraisemblable. Certains fraudeurs se servent de l'IA pour créer des messages, des images, des vidéos et des voix réalistes. Ils combinent parfois ces outils avec des informations trouvées en ligne pour personnaliser leur approche et la rendre plus crédible.

À titre d'exemple, l'IA peut servir à créer un message naturel et professionnel ou imiter la voix d'une personne que vous connaissez. Des images et des vidéos peuvent également être créées ou modifiées pour étayer un faux récit. Par conséquent, certains des indices qui servent habituellement à débusquer

la fraude, telle que des fautes d'orthographe, des formulations inhabituelles ou maladroites ou des images de mauvaise qualité, ne sont plus toujours présents.

En d'autres mots, un message, une image, une vidéo ou une voix qui semblent réels ne constituent pas pour autant une preuve d'authenticité.

Signaux d'alerte

Soyez prudent si :

- on vous pousse à agir immédiatement ou on vous menace de conséquences si vous ne le faites pas;
- on vous dit de garder le secret ou de ne pas en parler à votre famille, à vos amis, à votre institution financière ou à la police;
- on vous demande, de façon impromptue, de l'argent, des renseignements personnels ou financiers;
- on vous demande un mot de passe, un NIP ou un code de vérification à usage unique;
- vous êtes invité à cliquer sur un lien, à ouvrir une pièce jointe, à télécharger un logiciel ou à vous rendre sur un site Web que vous ne connaissez pas;
- une personne de votre entourage communique soudainement avec vous à partir d'un nouveau numéro de téléphone ou d'un nouveau compte et vous demande de l'argent;
- vous recevez subitement un prix ou un remboursement, ou une proposition d'investissement qui semble trop belle pour être vraie;
- vous recevez une demande inusitée, même si le message ou la personne semblent convaincants.

Comment vous protéger

- Marquez une pause. Ne laissez pas le sentiment d'urgence, la peur ou l'excitation vous pousser à agir rapidement.
- Faites des vérifications. Utilisez les coordonnées tirées d'une source fiable pour ce faire, et non celles fournies dans le message.
- Si une personne qui prétend être un membre de votre entourage communique avec vous, utilisez un numéro de téléphone que vous connaissez déjà pour vérifier qu'il s'agit bien d'elle.
- Ne vous fiez pas à l'identification de l'appelant. Le nom et le numéro qui s'affichent sur votre téléphone peuvent avoir été détournés.
- À moins d'être vous-même à l'origine de l'appel, ne fournissez jamais de mots de passe, de NIP ou de code de vérification à usage unique à un appelant.
- Évitez de cliquer sur des liens ou d'ouvrir des pièces jointes à des messages inattendus. Utilisez plutôt le site Web ou l'application officiels de l'organisme.
- Soyez prudent lorsque vous publiez de l'information en ligne. Pour être plus crédibles, les fraudeurs n'hésitent pas à utiliser des renseignements accessibles au public.
- Avant d'envoyer de l'argent ou de divulguer des renseignements de nature délicate, parlez-en à une personne de confiance.

Quiconque croit avoir été la cible de fraude ou de cybercriminalité est prié de le signaler à son service de police local, puis de faire un signalement en ligne sur le site Web Signaler la cybercriminalité et la fraude ou par téléphone au 1-888-495-8501.