LA FRAUDE EN 3D

Personne n'est à l'abri d'une escroquerie, peu importe son âge, son niveau de scolarité ou son lieu de résidence.

La plupart des fraudes peuvent être évitées. Pour cela, il faut savoir les reconnaître et être vigilant en se protégeant efficacement.

BANQUE DU CANADA
BANK OF CANADA

LA FRAUDE EST EN CONSTANTE ÉVOLUTION

RESTONS VIGILANTS

- Protéger ses informations personnelles en tout temps
- Examiner ses relevés bancaires de ses cartes de paiement
- Aviser la police et les institutions concernées de toutes transactions frauduleuses
- Consulter régulièrement son dossier de crédit auprès des agences d'évaluation du crédit
- Assurer la réception régulière de son courrier
- Bloquer les appels, courriels et messages textes frauduleux

POUR SIGNALER UNE FRAUDE

- Joindre votre service de police local ou la Sûreté du Québec au **310-4141** ou ***4141** (cellulaire)
- Contactez le Centre antifraude du Canada au **1 888 495-8501** ou **www.antifraudcentre.ca**

POUR EN SAVOIR PLUS

Téléchargez le livret *La Fraude en 3D* (version française ou anglaise) :

https://www.banqueducanada.ca/wp-content/uploads/2020/02/fraude-3d.pdf

https://www.bankofcanada.ca/wp-content/uploads/2020/02/fraud-3d.pdf

MISE EN GARDE – Vol par distraction

La Sûreté du Québec tient à vous mettre en garde contre un stratagème permettant à des fraudeurs de subtiliser des cartes de paiement à l'intérieur de véhicules (ou à même votre portemonnaie), en ayant recours à un scénario de distraction dans les stationnements de magasins à grande surface.

Le suspect et ses complices :

- Vous ciblent lors d'une transaction aux caisses en libre-service;
- Mémorisent le numéro d'identification personnel (NIP) de votre carte (crédit ou débit) en regardant par-dessus votre épaule :
    - Vous suivent jusque dans le stationnement et attendent que vous preniez place dans votre véhicule.
    - Tentent de vous distraire en vous interpellant afin que vous sortiez de votre véhicule (en prétextant qu'un montant ou qu'un portemonnaie au sol vous appartiendrait).
    - Un complice entre alors dans votre véhicule du côté passager pour subtiliser vos cartes de paiement (d'un sac à main laissé à la vue).
- Quittent les lieux pour procéder à des retraits à un guichet automatique ou pour acheter des cartes de crédit prépayées.

En l'absence de complice, le suspect vous demande de regarder dans votre portemonnaie s'il ne vous manque pas un billet de banque. Lorsque vous procédez à la vérification, le suspect dépose le billet sur votre portemonnaie et subtilise votre carte de paiement.

La Sûreté du Québec vous réitère l'importance de faire preuve de prudence et de vigilance :

- **Protégez votre NIP. Cachez-le du regard des autres personnes** lors de transactions.
- **Si vous êtes interpellé par un inconnu :**
    - ❖ **Demeurez dans votre véhicule.** Verrouillez vos portières. Baissez légèrement votre vitre.
    - ❖ Prenez connaissance de votre environnement (y a-t-il d'autres personnes autour de vous?).
    - ❖ Validez la demande (êtes-vous en possession de tous vos effets personnels?).
    - ❖ Dans le doute, proposez-lui de vous remettre l'article à travers l'ouverture de la vitre de votre portière. En cas de refus d'obtempérer, questionnez-vous, c'est probablement une arnaque.
- **Son insistance vous fait craindre pour votre sécurité**? Klaxonnez pour attirer l'attention ou quittez les lieux. Communiquez le plus rapidement possible avec votre service de police.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

- ❖ Service de police local ou Sûreté du Québec : 911
  *Municipalités non desservies par le 911: composer le 310-4141 ou *4141 (cellulaire)

- ❖ Communiquez avec le Centre antifraude du Canada au 1 888 495-8501

MISE EN GARDE – Arnaque au compte bancaire (JEUNES)

On vous offre une « solution facile » pour gagner de l'argent?
Faites preuve de prudence et de vigilance : l'argent facile, ça peut devenir compliqué.

La Division des enquêtes sur les crimes économiques de la Sûreté du Québec tient à mettre en garde les jeunes et leurs parents contre un stratagème où un fraudeur initie un contact avec sa jeune victime sur les médias sociaux, afin de lui faire miroiter la possibilité de gagner un montant d'argent très facilement.

Le fraudeur :

- explique à la victime qu'elle n'a qu'à lui « prêter son compte bancaire » en vue d'une transaction et ce, en échange d'une compensation financière.
- convainc la victime de lui transmettre ses informations bancaires, ses coordonnées personnelles et de lui remettre sa carte de débit.
- procède à un dépôt au compte de la victime (ex. virement ou photo de chèque).
- se rend au domicile de la victime pour récupérer sa carte de débit et tenter un retrait au guichet automatique.

Lorsque le retrait s'avère infructueux, la victime reçoit des **menaces** du fraudeur.

Un jeune qui participe à cette fraude verra son dossier entaché auprès de l'institution financière pour usage frauduleux d'un compte bancaire.

La Sûreté du Québec réitère l'importance de se méfier de toute « offre facile » pour gagner de l'argent. Soyez vigilant, c'est une arnaque.

- Ne prêtez jamais votre carte de débit ni ne divulguez vos informations bancaires (NIP).

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

- Service de police local ou Sûreté du Québec : 911
  *Municipalités non desservies par le 911: composer le 310-4141 ou *4141 (cellulaire)
- Communiquez avec le Centre antifraude du Canada au 1 888 495-8501

MISE EN GARDE – Rançongiciel

La Sûreté du Québec désire mettre en garde la population contre les attaques informatiques de type « rançongiciel ».

Qu'est-ce qu'un rançongiciel?

- Il s'agit d'un logiciel malveillant qui, lorsqu'il infecte un ordinateur, verrouille l'accès aux fichiers ou au système.
- Une demande de rançon, payable notamment par monnaie virtuelle (comme le *Bitcoin)*, apparaît à l'écran en échange de la clé de déchiffrement.
- L'ordinateur infecté reste généralement fonctionnel, mais les documents de travail ne sont pas utilisables.
- L'utilisateur se retrouve incapable de les ouvrir avec les logiciels habituels.

Exemple de message apparaissant à l'écran :

All your files have been encrypted!

Comment les cybercriminels s'y prennent-ils ?

Ils utilisent l'exploitation du service de bureau à distance de Windows, en misant principalement sur la faiblesse du mot de passe afin de se connecter au service qui leur donne le contrôle de l'appareil et leur permet d'y installer eux-mêmes le logiciel malveillant.

Lorsque le rançongiciel est installé, les cybercriminels peuvent exécuter d'autres actions sur le système telles qu'installer d'autres programmes, désactiver l'antivirus, effacer les journaux d'événements, etc.

Les rançongiciels sont aussi transmis par l'entremise de pièces jointes de courriels ou encore, lorsque l'utilisateur clique sur un lien qui le redirige vers des sites web contrôlés par les cybercriminels.

Comment prévenir les attaques par rançongiciels?

- **Sensibiliser les employés de manière active :** leur indiquer d'éviter de cliquer sur un lien ou d'ouvrir un fichier d'origine inconnue dans un courriel ou un texto. Toujours demander l'aide des techniciens attitrés et éviter les solutions de type « technicien en ligne ».
- **Effectuer les mises à jour régulièrement :** la plupart des rançongiciels exploitent des failles que l'on peut éviter.
- **Avoir une solution de sécurité complète qui offre une protection contre les rançongiciels, les pourriels et la navigation Web.**
- **Sécuriser le service de bureau à distance :** utiliser des services d'accès à distance sécurisés tels que des « VPN » qui exigent la double authentification et des mots de passe robustes.
- **Limiter l'utilisation de comptes de type administrateur sous Windows.**
- **Instaurer une procédure de sauvegarde** : tenir compte de la fréquence des sauvegardes en fonction de la nature et de la valeur des données, et s'assurer que les sauvegardes sont stockées à l'extérieur du réseau commun. Si vous êtes victime d'un rançongiciel, votre sauvegarde risque d'être votre seule solution.

Quoi faire si vous êtes victime d'un rançongiciel?

Ne pas payer la rançon. Le paiement de la rançon ne garantit pas la récupération des données et encourage la récidive.

POUR SIGNALER CE TYPE D'ÉVÉNEMENT, COMMUNIQUER AVEC :

- **La Sûreté du Québec au 9-1-1**
  *Municipalités non desservies par le 9-1-1: composer le 310-4141 ou *4141 (cellulaire)

- **Votre service de police local.**