Attention, stratagème de fraude en cours actuellement sous forme d'HAMEÇONNAGE (PHISHING)

Aux KRTB comme un peu partout au Québec en ce moment, des gens inquiets nous appellent après avoir un reçu un courriel leur laissant croire qu'ils sont sous enquête policière et qu'afin de régulariser leur situation, ils doivent cliquer sur un lien qui les amènent vers un formulaire à compléter dans lequel on vous demande vos renseignements personnels.

Sachez qu'il s'agit d'un stratagème frauduleux dans le but d'obtenir du renseignement personnel (date de naissance, numéro de carte de crédit, renseignements bancaires, mots de passe, numéro d'assurance sociale) en faisant croire aux victimes que la communication provient d'une entité légitime (entreprise, institution financière, organisme gouvernemental ou policière). Plusieurs techniques peuvent être employées par les fraudeurs afin de soutirer ces informations, telles que l'envoi d'un faux courriel reproduisant le contenu d'un message authentique avec des indications pour obtenir des renseignements personnels ou d'un faux message texte avec un hyperlien frauduleux renvoyant les victimes vers un site Web factice qui semble familier pour soutirer les renseignements personnels des victimes. L'hameçonnage peut ainsi mener à une fraude d'identité

COMMENT SE PROTÉGER?

- Sachez qu'un organisme fiable ne demande jamais de renseignements personnels par courriel ou texto.
- N'ouvrez que les courriels ou messages provenant d'un destinataire en qui vous avez confiance et téléchargez seulement les fichiers Internet qui proviennent de source sûre.
- Ignorez les courriels et messages textes de personnes inconnues.
- Supprimez les messages suspects; ceux-ci peuvent contenir des virus.
- Supprimez vos pourriels; n'ouvrez pas les pièces jointes et ne cliquez pas sur les hyperliens.
- Mettez à jour l'antivirus de tous vos appareils.
- N'utilisez jamais le numéro de téléphone ou l'adresse courriel fournis dans un message suspect; faites une recherche en ligne pour identifier ces renseignements sur les sites Web officiels.
- Vérifiez régulièrement vos relevés bancaires.
- Assurez-vous de la présence du petit cadenas dans la barre d'adresse lors de vos navigations en ligne; celui-ci assure que la connexion au site Web est sécurisée.
- Vérifiez que l'adresse du site Internet débute par « https:// »,?
- Assurez-vous que l'adresse du site est bel et bien celle que vous avez l'habitude d'utiliser (par exemple : http://www.desjardins.com par rapport à http://www.desjardins1.com).

POUR SIGNALER UNE FRAUDE OU CONNAITRE LES STRATAGÈMES FRAUDULEUX EN COURS, CONTACTEZ LE CENTRE ANTIFRAUDE DU CANADA.

https://antifraudcentre-centreantifraude.ca/report-signalez-fra.htm ou composez le 1 888 495-8501

POUR OBTENIR DE L'AIDE

Communiquez avec la Sûreté du Québec au **310-4141 ou *4141 (cellulaire**) ou votre service de police local.

Consultez la fiche « Dépôt d'une plainte pour fraude - aide-mémoire citoyen » sur le site web de la Sûreté du Québec; https://www.sq.gouv.qc.ca/wp-content/uploads/2021/01/sq-3616.pdf
Bonne journée