MARS, *MOIS DE PRÉVENTION DE LA FRAUDE*

Tout au long du mois de mars, à l'occasion du *Mois de prévention de la fraude*, la Sûreté du Québec et plusieurs partenaires des forces policières, en collaboration avec la Banque du Canada, mènent une campagne afin de sensibiliser les citoyens aux différents types de fraudes les plus courantes.

Personne n'est à l'abri de la fraude, peu importe son âge, son niveau d'éducation ou son lieu de résidence. Cependant, la plupart des fraudes peuvent être évitées en étant informé et vigilant afin de les identifier et se protéger efficacement.

FRAUDES LIÉES AUX CRYPTOMONNAIES

Il s'agit de stratagèmes ayant recours aux monnaies numériques ou virtuelles, qui se présentent sous la forme de codes cryptographiques (cryptés).

Les fraudeurs profitent de la difficulté à retracer une cryptomonnaie afin :

- de se faire passer pour un individu (ex. employé du gouvernement) afin de soutirer à une victime un montant d'argent sous la forme de cryptomonnaie (ex. bitcoin).
- de créer de fausses plateformes d'échange de cryptomonnaies, afin de subtiliser un montant aux victimes.
- de créer des faux portefeuilles virtuels facilitant l'application d'un rançongiciel ou qui imitent des sites populaires afin de subtiliser un montant aux victimes.
- d'exiger un paiement avec de la cryptomonnaie pour un faux achat en ligne (le produit ne sera jamais livré).
- d'inciter les investisseurs à participer à de faux placements dans des émissions de cryptomonnaie ou de jeton, communément appelées « ICO » (Initial coin offering) qui sont rattachées à de soi-disant projets technologiques en démarrage.

Comment font les fraudeurs ?

- En promettant des taux de rendement incroyables et un service à la clientèle impeccable, les arnaqueurs réussissent à convaincre les victimes que leur plateforme d'échange ou leur première émission de cryptomonnaies est supérieure.
- En communiquant directement avec la victime par téléphone, texto ou courriel, et la menacer (ex. d'impôt non payé), afin d'exiger un paiement immédiat en cryptomonnaie.
- En imitant certains sites de transactions sur internet afin de duper les victimes.

Comment se protéger ?

- Vérifiez constamment la légitimité de l'interlocuteur lors des transactions (en personne, par téléphone, par courriel, par Internet, etc.) : retrouvez le numéro de téléphone officiel de l'organisme qui vous a contacté et vérifiez la validité de la demande qui vous est adressée. Utilisez des sites sécurisés (débutant par « https:// »).
- Validez l'adresse courriel de l'expéditeur dans toutes vos communications. Interrogez-vous toujours avant de cliquer sur un lien ou d'ouvrir un fichier d'origine inconnue. Ne répondez jamais

à des courriels où l'on vous demande de valider vos informations personnelles ou encore de confirmer votre nom d'utilisateur ou votre mot de passe.

- Demeurez vigilant devant toutes les transactions en ligne avec des cryptomonnaies. Attention aux plateformes qui conservent les clés privées lors d'achats, c'est une arnaque.
- Vérifiez la source de téléchargement des portemonnaies pour ne pas inviter un virus dans vos systèmes informatiques.
- Privilégiez un ou plusieurs portemonnaies physiques pour conserver votre cryptomonnaie.
- Préservez vos renseignements personnels et ne partagez jamais vos clés privées avec une autre personne.
- Conservez tous documents relatifs aux transactions de cryptomonnaies.

RANÇONGICIELS

C'est quoi?

- 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. On peut aussi vous inviter à contacter un faux technicien de Microsoft.

Comment se protéger?

- Évitez de cliquer sur un lien ou d'ouvrir un fichier d'origine inconnue dans un courriel ou un texto. Demander l'aide des techniciens attitrés (le cas échéant) et éviter les solutions de type « technicien en ligne ».
- Effectuez les mises à jour régulièrement du système d'exploitation de votre ordinateur : la plupart des rançongiciels exploitent des failles que l'on peut éviter.
- Ayez 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 » (Virtual Private Network) qui exigent la double authentification et des mots de passe robustes (frais exigés).
- Limitez l'utilisation de plusieurs comptes de type administrateur sous Windows.
- Instaurez 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.
- Sensibilisez les autres utilisateurs de votre réseau si celui-ci est partagé. (ex. : Famille utilisant le même Wi-Fi à la maison).

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 OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

Si vous soupçonnez ou savez avoir été victime d'une fraude liée aux cryptomonnaies, signalez l'incident :

- auprès de votre service de police local.
- au Centre antifraude du Canada au 1 888 495-8501 ou au www.antifraudcentre-centreantifraude.ca.

Mars, Mois de prévention de la fraude.
Un mois de prévention, douze mois de vigilance!