



COMMUNIQUÉ DE PRESSE

RÉGIE INTERMUNICIPALE DE POLICE ROUSSILLON

Extorsion, alerte à la fraude!

CANDIAC, le 20 mars 2024 – En ce mois de prévention de la fraude, la Régie intermunicipale de police Roussillon invite les citoyens à la vigilance concernant l'extorsion.

L'extorsion est le fait qu'une personne, sans excuse raisonnable et sans justification dans le but d'obtenir quelque chose, par menaces, accusations ou violence, induise ou tente d'induire une personne à accomplir ou à faire accomplir quelque chose. Il y a extorsion lorsqu'une personne obtient illégalement de l'argent, des biens ou des services d'une personne, d'une entité ou d'une institution par la coercition.

Voici quelques exemples d'extorsion utilisée par les fraudeurs

Vidéo explicite

Dans un courriel, un fraudeur prétend avoir piraté votre ordinateur et vous avoir enregistré en train de vous livrer à un acte explicite (ex. en train de vous masturber). Souvent, il vous donnera certains de vos renseignements personnels (ex. votre numéro d'assurance sociale) ou un mot de passe que vous avez déjà utilisé pour prouver qu'il a piraté votre ordinateur. Il affirme que la vidéo sera rendue publique si vous ne le payez pas en bitcoins immédiatement.

L'ordinateur n'a pas été piraté. Le mot de passe cité a été obtenu dans un piratage antérieur.

Services d'électricité

Un fraudeur prétend être un employé de votre compagnie d'électricité. Il affirme que vous ou votre entreprise avez un solde impayé sur votre compte d'électricité et que vous devez le payer immédiatement, à défaut de quoi la compagnie coupera le courant.

Le fraudeur peut demander que le paiement soit fait par l'intermédiaire d'une entreprise de transfert de fonds, par carte de crédit prépayée ou par carte-cadeau (iTunes, Google Play ou Steam), ou par bitcoin.

La cryptomonnaie est un actif numérique, ou virtuel, qui peut être échangé contre des biens et des services. Rappelez-vous: **les transactions bitcoin sont irréversibles**

Communiqué: 2024-006



COMMUNIQUÉ DE PRESSE

RÉGIE INTERMUNICIPALE DE POLICE ROUSSILLON

Organisme d'application de la loi

Vous recevez un courriel ou un appel provenant supposément d'un organisme d'application de la loi, comme la GRC, Interpol ou Europol. Les fraudeurs utiliseront des logos de services de police ou d'autres identifiants pour paraître légitimes. Vous pourriez recevoir :

- Une lettre frauduleuse vous informant que vous faites l'objet d'accusations criminelles graves et vous demandant de communiquer avec eux pour éviter la prison;
- Un message dans lequel les fraudeurs vous demandent d'envoyer de l'argent pour éviter d'être arrêté;
- Un courriel avec une pièce jointe malveillante que les fraudeurs vous demanderont d'ouvrir.

D'autres exemples d'extorsion sont aussi disponibles sur le site internet du **Centre Antifraude du Canada** au <https://antifraudcentre-centreantifraude.ca/scams-fraudes/extortion-extorsion-fra.htm>

Quiconque croit avoir été victime d'un acte de cybercriminalité ou de fraude doit le signaler à la Régie intermunicipale de police Roussillon et au CAFC au moyen de son système de signalement en ligne ou par téléphone au 1 888 495-8501. Tout incident de cette nature doit être signalé au CAFC.

Sources :

- Centre antifraude du Canada
- InstacoinATM

-30-

Section relations médiatiques
514 918-4483

Communiqué: 2024-006

Page 2