Bulletin sur les tendances de la criminalité financière :

Fraude par échange de carte SIM

2019-11-01

La fraude : Identifiez-la. Signalez-la. Enrayez-la.

#DéNONcerlaFRAUDE

Objet

Le présent bulletin a pour but d'informer les consommateurs sur les précautions à prendre en ce qui concerne la fraude par échange de carte SIM.

Aperçu

Les fraudeurs se servent de la fraude par échange de carte SIM et transfert de numéro de téléphone pour accéder à vos comptes financiers, de courriel et des médias sociaux. Par la suite, ils accèdent directement à vos renseignements personnels, votre calendrier, vos contacts, votre argent et même plus. Les fraudeurs peuvent vider vos comptes bancaires, présenter une demande de crédit en votre nom ou se faire passer pour vous afin de flouer tous vos contacts. Vous perdez ainsi l'accès à votre service mobile, n'arrivez plus habituellement à ouvrir de sessions pour vos comptes et êtes pris au dépourvu.

Voici comment cette fraude fonctionne :

Votre carte SIM établit un lien entre votre appareil et votre numéro de téléphone et votre service sans fil. Vous vous servez ensuite de votre appareil mobile pour vous connecter à de nombreux de comptes à l'aide de diverses applications. La plupart des identifiants de connexion sont liés à votre courriel, à votre numéro de téléphone ou aux deux (si vous configurez l'authentification à deux facteurs).

Un fraudeur se fera passer pour vous pour accéder à votre compte de service sans fil et prétendra que votre téléphone a été perdu ou volé. Votre numéro de téléphone sera alors associé à une nouvelle carte SIM et à un nouvel appareil contrôlé par le fraudeur, qui lui téléchargera les applications les plus utilisées et intéressantes. Il cliquera sur le lien ou le bouton « Mot de passe oublié » de toutes les applications. Si un compte est associé à votre numéro de téléphone ou à votre courriel, le fraudeur recevra un code de vérification qu'il utilisera ensuite pour confirmer que celui-ci lui appartient. Il créera son propre mot de passe et en prendra le contrôle.

Indices – Comment vous protéger

- Gardez vos renseignements personnels confidentiels. Ça peut être aussi simple que de ne pas publier votre date de naissance dans les médias sociaux.
- Ne répondez pas aux courriels ou aux textos d'hameçonnage dans lesquels on vous demande de confirmer votre mot de passe ou de mettre à jour les renseignements de votre compte.
- Utilisez un gestionnaire de mots de passe hors ligne.
- Communiquez avec votre fournisseur de service sans fil et demandez-lui quelles sont les autres mesures de sécurité pouvant être appliquées à votre compte.
- Si vous perdez votre service sans fil, communiquez immédiatement avec votre fournisseur de service.

Si vous croyez être victime de fraude ou si vous connaissez une personne qui a été victime de fraude, communiquez avec le Centre antifraude du Canada au 1-888-495-8501 ou rendez-vous au http://www.centreantifraude.ca.