BULLETIN DU CENTRE ANTIFRAUDE DU CANADA

Mois de la littératie financière : Fraude avec codes QR 2023-11-08

LA FRAUDE : IDENTIFIEZ-LA, SIGNALEZ-LA, ENRAYEZ-LA

Novembre est le Mois de la littératie financière, et le Centre antifraude du Canada (CAFC) y contribue en publiant le présent bulletin d'information à l'intention du grand public.

Le CAFC reçoit des plaintes selon lesquelles des fraudeurs utilisent des codes QR pour voler des renseignements personnels et de l'argent. Ces codes, tout comme les liens hypertextes et les adresses URL, sont insérés dans des courriels et des textes et mènent à des sites Web frauduleux ou malveillants. Voici quelques-unes des variantes que le CAFC a observées :

Hameçonnage

Un fraudeur prétend être un fournisseur de services, un organisme gouvernemental ou une institution financière et au lieu de demander à la victime de cliquer sur un lien ou de télécharger une pièce jointe, il lui demande de scanner un code QR.

Fraude liée à la vente

Les fraudeurs s'en prennent à des personnes vendant des articles. Pour donner l'illusion de les payer, ils leur envoient un code QR qu'elles doivent scanner, après quoi, elles se font demander leurs renseignements bancaires en ligne. Elles courent ainsi le risque de se faire usurper leur identité.

Dans une autre variante, les fraudeurs envoient un code QR aux victimes en prétendant leur envoyer un paiement, alors qu'en réalité, ils demandent de se faire payer. Si une victime saisit ses renseignements bancaires, le fraudeur reçoit son paiement ou peut accéder à son compte bancaire.

Cryptomonnaie

Les fraudeurs profitent du manque général de connaissances des Canadiens en matière de cryptomonnaie. Dans de nombreux types de fraudes, ils demandent un paiement dans ce type de monnaie. Bien souvent, ils envoient une adresse sous forme de code QR que les victimes sont invitées à scanner pour effectuer un paiement. Au final, l'argent est envoyé dans des portefeuilles de cryptomonnaie contrôlés par les fraudeurs.

Indices – Comment vous protéger

- Méfiez-vous des messages textes, courriels et messages sur les médias sociaux que vous n'avez pas sollicités et qui vous demandent de scanner un code QR.

- Survolez le code QR avec la caméra de votre appareil, sans vous rendre sur le site Web. Cela fait souvent apparaître l'adresse URL ou le lien hypertexte frauduleux associé au code. L'adresse URL peut révéler un nom ou un titre illégitime.
- Si vous scannez un code QR et acceptez d'ouvrir le lien qui s'y rattache, sachez que vous courez le risque d'infecter votre appareil ou le réseau de votre organisation, ou de vous faire usurper votre identité.
- Si vous êtes invité à scanner un code QR pour consulter un document, communiquez avec le service informatique de votre organisation pour vous assurer que cela ne mettra pas en danger son réseau ou ses systèmes.
- Si vous vendez un article, ne scannez jamais un code QR pour vous faire payer. En cas de doute, communiquez directement avec la société offrant des services de paiement.
- Sachez qu'aucun organisme du gouvernement n'exige de paiement en cryptomonnaie, en aucune circonstance.
- N'oubliez pas que les paiements en cryptomonnaie sont presque impossibles à retracer!
- Autres conseils et trucs pour vous protéger.

Si vous pensez avoir été victime de cybercriminalité ou de fraude, signalez-la à votre service de police local et au système de signalement en ligne du Centre antifraude du Canada (CAFC) ou par téléphone au 1-888-495-8501. Si un incident s'est produit, mais que vous n'êtes pas tombé dans le piège, signalez-le tout de même au CAFC.