CANADIAN ANTI-FRAUD CENTRE BULLETIN

Financial Literacy Month: QR Code Fraud 2023-11-08

FRAUD: RECOGNIZE, REJECT, REPORT

This bulletin was prepared to inform the public as part of the Canadian Anti-Fraud Centre's contribution for this November's Financial Literacy Month.

The CAFC is receiving reports of fraudsters using QR codes in various scams to steal your personal information and/or money. Similar to fraudulent links or URLs, QR codes can be inserted into emails and texts to direct potential victims to fraudulent or malicious websites. Below are some of the variations we have seen:

Phishing with QR Codes

Fraudsters may claim to be a service provider, government agency, or financial institution. Instead of asking the victim to click on a link or download an attachment, fraudsters will instruct the victim to scan a QR code.

Vendor Fraud

Victims selling items are being targeted by QR code fraud. Fraudsters will send a fake payment advising that the victim must scan the QR code in order to receive a payment. If the victim scans the QR code, they will be asked for their online banking information putting them at risk for identity fraud.

In another variation, fraudsters will send a QR code to the victim claiming that they are sending a payment but, in reality it is a request for a payment. When the victim enters their banking information, fraudsters will receive the payment or may gain access to the victim's bank account.

Cryptocurrency QR Codes

Fraudsters are taking advantage of Canadians' general lack of knowledge related to crypto currency. Fraudsters will ask for crypto currency as a payment in many different types of fraud. In many cases, fraudsters will send a crypto currency address in the form of a QR code. Victims are then directed to scan it to make a payment. In the end, payments will be sent to crypto wallets controlled by the fraudsters.

Warning signs – How to protect yourself

- Beware of unsolicited text messages, emails, and social media messages asking you to scan a QR Code.

- Hovering over the QR code with a device camera, without agreeing to proceed to the website, will often show the fraudulent link/URL associated with the code. The URL may indicate an illegitimate name or title.
- Scanning a QR code and agreeing to follow the associated link can potentially put you at risk for identity fraud and can potentially infect your device or business network.
- If a request is received to view a document by scanning a QR code, contact your IT department before putting the network/business systems at risk.
- If you are selling an item, never scan a QR code to receive a payment. If you are unsure, contact the payment service company directly to confirm.
- No government agency will demand payment via crypto currency under any circumstances.
- Remember, crypto payments are nearly untraceable!
- Learn more tips and tricks for protecting yourself.

If you suspect you have been the victim of cybercrime or fraud report it to your local police and to the Canadian Anti-Fraud Centre's online reporting system or by phone at 1-888-495-8501. If not a victim, report it to the Canadian Anti-Fraud Centre anyway.