CANADIAN ANTI-FRAUD CENTRE BULLETIN

Social Media Fraud 2024-10-15

FRAUD: RECOGNIZE, REJECT, REPORT

With more people than ever communicating and socializing online, the CAFC wants to help keep you safe from fraud on social media as part of Cybersecurity Awareness Month. From having your account compromised to falling for an investment fraud, these scams can be costly if you're not vigilant.

Common Social Media Scams:

Account compromise frauds

Have you received an offer from friend for a good deal on Taylor Swift concert tickets or requests for assistance from a family member that lost their phone or have you responded to immigration offers promoted by Canadian members of parliament?

Beware, fraudsters are increasingly compromising profiles on social platforms like Facebook. These accounts are then used to promote frauds including merchandise scams, emergency scams and even immigration scams.

Investment Scams

There are two very prominent online investment frauds to be aware of.

- In celebrity endorsed investment frauds, perpetrators create and post fake news articles using deepfake videos of well-known high-profile figures to lure victims into crypto currency investing.

- In relationship investment frauds, perpetrators will contact you via online dating sites, social media platforms and even by text messages attempting to start a relationship and build trust with you. They typically claim to be successful cryptocurrency investors and persuade you to invest with the promise of high returns.

Sextortion

Fraudsters are creating fake profiles on social media, pornographic and dating websites. They use these to lure you into a relationship and coerce you into performing sexual acts on camera. Sextortion, or online sexual exploitation, is blackmail. It occurs when someone threatens to send an existing (or fabricated) sexual image or video of you to other people if you do not pay them or provide more sexual content. It can also occur when someone is encouraged to participate in or observe online situations of a sexual nature. These encounters can be recorded or captured without the victim's knowledge. The fraudster then threatens to send the recorded material to friends, family members, or work colleagues if money or additional images are not sent.

Warning signs for all variations

• Someone you haven't met in person professes their love to you.
• Unsolicited text messages from people you don't know.
• A suspect that tries to move communication to a more private or different method of communication (Whatsapp, Signal or Discord, etc.)
• Any attempts to meet in person get cancelled or there's always an excuse to not meet up.
• A suspect acting distressed or angry to force you into sending more money.
• Friend requests from people you don't know or profiles that seem too perfect.
• Requests for remote access to your device in order to "teach" you how to invest.
• Investment opportunities with higher than normal returns.
• Requests to transfer your crypto investment to an alternate crypto address.
• Investment Ads using high profile individuals promising a high return on your investment.

How to protect yourself from all variations

• Don't accept friend requests from people you do not know.
• Be careful who you share images with. Suspects will often use explicit pictures to extort victims into sending money.
• Lean more tips on how to protect yourself from Sextortion
• Never send money to someone you haven't met.
• Don't give out your personal information (name, address, DOB, SIN, banking credentials).
• Never scan a QR code provided by an unknown source. It could contain a virus and infect your device.
• Don't allow remote access to your device (Anydesk, Teamviewer, etc..).
• Be careful when sending cryptocurrency; once the transaction is completed, it is unlikely to be reversed.
• Verify if the investment companies are registered the National Registration Search Tool www.aretheyregistered.ca
• Beware of fraudsters asking you to open and fund new crypto accounts. They will direct you to send it to addresses they control. Don't!
• Beware of offers promising high returns on investments. If it's too good to be true, it most likely is!
• Learn more tips and tricks for protecting yourself.

If you think you or someone you know has been a victim of fraud, please contact the Canadian Anti-Fraud Centre at 1-888-495-8501 or report online at www.antifraudcentre-centreantifraude.ca.