CANADIAN ANTI-FRAUD CENTRE BULLETIN

Online Extortion 2023-10-30

FRAUD: RECOGNIZE, REJECT, REPORT

This bulletin was prepared to inform the public as a part of Canadian Anti-Fraud Centre's (CAFC) campaign for this October's Cyber Month.

Extortion continues to be one of most common tactics fraudsters use in frauds. Extortion happens when someone unlawfully obtains money, property or services from a person, entity or institution through coercion.

The CAFC would like to warn the public about the most common variations of online extortion frauds.

Extortion email featuring password:
Canadians are receiving a threatening email from an unfamiliar contact. The email claims to have gained access to the recipient's computer, installed malware and recorded an explicit video of the recipient. The email sender threatens to send the video to the recipient's contacts, if they do not pay money via bitcoin immediately. The fraudsters apply pressure on the recipient by setting a short time limit.

These fraudulent emails attempt to prove the legitimacy of their claims by including one of the recipient's passwords. In many cases, the password is being confirmed by recipients as an old password. These passwords were likely collected during previous frauds. (e.g. phishing scam or database breach).

Fake law enforcement extortion email:
Canadians are receiving threatening emails claiming to be from international law enforcement agencies, but most commonly the RCMP. The fraudulent email asks you to open an attachment to view the fraudulent letter. After opening the attachment, a letter using law enforcement logos, names of high-ranking law enforcement officials is displayed and claims that you are accused of serious criminal charges. Suspects provide a fake law enforcement email address to respond to. After communicating with suspects, they will ask you to send a payment to avoid going to jail.

Social media crypto extortion:
Fraudsters are sending phishing emails with fraudulent links for fake Instagram login pages; this allows fraudsters to steal account credentials. Once an account is taken over, suspects blackmail victims to record a video of themselves promoting fake crypto currency platforms. Suspects advise victims that this is the only way they can recover their account. After the video is recorded, it is posted on the victim's social media accounts with a link that connects their followers with fraudulent investment platforms. Victims will never recover their social media account and their followers are at risk of losing their funds if they invest through the fraudulent crypto currency platform

Sextortion:
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.

Social media can allow fraudsters to develop an understanding of someone's social circles and enable communication between threat actors and potential victims. Social media platforms are commonly used in sextortion.

In 2022, the CAFC observed more reports of sextortion targeting teenagers and younger victims, particularly through online video games, chat groups and social media. Threat actors may impersonate a younger individual to slowly develop trust or begin a virtual relationship. Like extortion and other forms of fraud, sextortion can be isolating and traumatic. This uncomfortable experience can force the victim to pay the fraudster and be afraid of reporting or telling a parent or guardian. Unfortunately, payment is never a solution. Once someone pays, they will be further targeted with continued threats.

As this form of fraud is targeting young Canadians and teenagers, it is important that parents and children develop an understanding of this online threat.

Warning signs – How to protect yourself from online extortion

- Do not open unsolicited emails.
- If an email contains one of your passwords, change it immediately.
- Always use a different password for every account.
- Law Enforcement will never threaten you by email and will not demand a payment
- Beware of unsolicited text messages and emails from individuals or organizations asking you to click on a link or attachment
- Do not download attachments as these can contain viruses or malware that may infect your device
- Contact the agency directly to verify the legitimacy
- Beware of fraudulent cryptocurrency investment advertisements promoted through social media.
- Prior to investing, ask for information on the investment. Research the team behind the offering and analyze the feasibility of the project.
- Enable multi-factor authentication as an added layer of protection for your online accounts.
- Recognize that live streaming can be recorded and that pre-recorded video can be livestreamed.
- Familiarize yourself with social media privacy settings and consider limiting who has access to your personal information (i.e. friends list, location).
- Unless you know the person offline, there is no way to confirm who is on the other end.
- Trust your instincts, be skeptical and cautious.
- Never send money to someone you haven't met.
- Avoid sharing intimate images online

- Don’t get sextorted, send a naked mole rat (www.dontgetsextorted.ca) thanks to CyberTip.ca, a program of the Canadian Centre for Child Protection.
- Learn more and protect yourself from sextortion
- Learn more tips and tricks for protecting yourself.

Anyone who suspects they have been the victim of cybercrime or fraud should report it to their local police and to the CAFC’s online reporting system or by phone at 1-888-495-8501. If not a victim, report it to the CAFC anyway.

For instances of sextortion involving youth under 18, please also report to www.cybertip.ca. Cybertip.ca is Canada’s tip line for reporting online child sexual abuse and exploitation and dedicated to reducing child victimization through technology, education, public awareness, along with supporting survivors and their families.

The CAFC is updating the fraud and cybercrime reporting statistics available on the Open Government Portal. Check out the portal today to see statistics up to September 30, 2023.