CANADIAN ANTI-FRAUD CENTRE BULLETIN

Extortion Email Alert! 2024-09-19

FRAUD: RECOGNIZE, REJECT, REPORT

The Canadian Anti-Fraud Centre is receiving reports of various extortion letters received via email. The extortion letters contain the full name, personal telephone number, personal residential address as well a screenshot from search engines of the recipient's residence. The extortion letter claims that the recipient has visited explicit websites and threatens to send a copy of a video to the recipient's contact list unless payment via cryptocurrency is made. A variation of the letter contains a QR Code.

Based on the reports received, victims have not used the service which fraudsters are mentioning. Similar to other extortion scams, fraudsters are attempting to scare victims into sending funds. Extortion scams are defined as "*when someone unlawfully obtains money, property or services from a person, entity, or institution through coercion*".

Safety Recommendations

- Do not scan QR Codes provided by an unknown source. They could infect your device.
- If you received a message threatening, report it to your local police immediately.
- Remember that fraudsters use high-pressure intimidation tactics to try to steal your money.
- Ensure that your social media profiles are at the highest privacy levels
- Limit sharing personal details on social media
- Should you believe any of your personal information has been compromised, you are encouraged to contact Equifax and TransUnion to flag your accounts.
- Be suspicious of any unsolicited messages or social media requests including those that are threatening or accuse you of owing money for a service you never used or planned to have.
- Do not send money under pressure.
- Do not reply to threatening messages.
- Learn more tips on how to protect yourself.

Anyone who has received a similar violent extortion message should report it to their local police immediately. After contacting local police, it is important to report the incident to the Canadian Anti-Fraud Centre's via its online reporting system or by phone at 1-888-495-8501. If you are not a victim, it is still important to report the incident to the CAFC. Reporting can prevent further harm.

[redacted]

I know that calling [redacted] would be a convenient way to contact you if you don't act. Don't try to hide from this. You have no idea what I'm capable of in [redacted]

It's important you pay attention to this message right now. Take a moment to chill, breathe, and analyze it thoroughly. 'Cause we're about to discuss a deal between you and me, and I ain't playing games. You don't know me but I know EVERYTHING about you and right now, you are wondering how, right?

Well, you've been a bit careless lately, scrolling through those videos and venturing into the darker corners of cyberspace. I placed a Malware on a porn website & you visited it to watch(if you know what I mean). While you were busy watching videos, your device initiated operating as a RDP (Remote Control) which provided me with total control over your device. I can look at everything on your display, flick on your camera and mic, and you wouldn't even notice. Oh, and I've got access to all your emails, contacts, and social media accounts too.

Been keeping tabs on your pathetic life for a while now. It is simply your misfortune that I stumbled across your bad deeds. I invested in more time than I should have exploring into your data. Extracted quite a bit of juicy info from your system. and I've seen it all. Yeah, Yeah, I've got footage of you doing filthy things in your room (nice setup, by the way). I then developed videos and screenshots where on one side of the screen, there's the videos you were enjoying, and on the other part, it is someone jerking off. With simply a single click, I can send this filth to every single of your contacts.

Your confusion is clear, but don't expect sympathy. Wholeheartedly, I'm ready to wipe the slate clean, and allow you to move on with your life and wipe your slate clean. I will give you two alternatives.
Option One is to turn a deaf ear this email. You should know what will happen if you opt this option. I will send your video to all of your contacts. The video was lit, and I can't even fathom the humiliation you'll face when your colleagues, friends, and fam see it. But hey, that's life, ain't it? Don't be playing the victim here.

Second wise option is to pay me, and be confidential about it. We will call this my "keep the secret charges". Lets discuss what happens when you select this option. Your dirty secret will remain your secret. I will wipe everything clean once you send payment. You will make the payment via Bitcoin only. Pay attention, I'm telling you straight: 'We gotta make a deal'. I want you to know I'm coming at you with good intentions. My word is my bond.

Amount to be paid: USD 2000
BTC ADDRESS IS: [redacted]
Or, (Here's your Bitcoin QR code, you can scan it):

[redacted]

Let me tell ya, it's peanuts for your peace.

Notice: You got one day to sort this out and I will only accept Bitcoins (I've a specific pixel in this email, and right now I know that you've read this e-mail). My system will catch that Bitcoin payment and wipe out all the dirt I got on you. Don't even think about replying to this or negotiating, it's pointless. The email and wallet are custom-made for you, untraceable. If I notice that you've shared or discussed this email with someone else, your garbage will instantly start getting sent to your contacts. And don't even think about turning off your phone or resetting it to factory settings. It's pointless. I don't make mistakes, [redacted]