CANADIAN ANTI-FRAUD CENTRE BULLETIN

Alert: Bank Investigator New Variations 2022-08-24

FRAUD: RECOGNIZE, REJECT, REPORT

The Canadian Anti-Fraud Centre continues to receive reports from victims who have been contacted by fraudsters claiming to be from a financial institution, law enforcement or an online merchant. Suspects claim that there have been suspicious and unauthorized charges on your credit card or funds have been stolen out of your bank account. They then state they need your credit card or bank card information including PIN number to stop the fraud.

In some cases, scammers will request access to the victims' computer to continue the "investigation". Victims are then shown a fraudulent transaction on their online bank account. The scammers state they want the victims' help in an ongoing "investigation" against the criminals who stole their money and request that the victims send funds as part of the "investigation".

*****New Variations*****

Two recent variation of this scam include:

1) Victims are directed to dial *72 followed by a phone number. *72 is used to forward any calls to the victim's phone number to an alternate phone number. If *72 is dialed by the victim, suspects will receive all incoming calls including legitimate financial institution phone calls that may potentially flag actual fraudulent charges by the suspects.

2) Fraudsters go to the victim's residence in person to pick up their bank cards. Some recent reporting identified victims being directed to put their bank card and PIN number in an envelope and place on their front steps for pick-up by an "investigator". Fraudsters retrieve the card and proceed to complete unauthorized transactions.

Warning Signs – How to Protect Yourself

- Don't dial *72; it will forward all incoming phone calls to the fraudsters.
- Fraudsters will often provide the first 4 numbers of your debit or credit card. Remember that most debit and credit card numbers with specific financial institutions begin with the same 4 numbers.
- Calls from Bank Investigator fraudsters tend to happen early in the morning when a victim is still sleeping or not alert.
- Financial institutions or online merchants will never request transferring funds to an external account for security reasons.

- Financial institutions or police will never request you to turn over your bank card nor attend your residence to pick up your bank card.
- Criminals use Call-Spoofing to mislead victims. Do not assume that phone numbers appearing on your call display are accurate.
- Never provide remote access to your computer.
- If you get an incoming call claiming to be from your financial institution, advise the caller that you will call them back. End the call and dial the number on the back of your card from a different phone if possible or wait 10 minutes before making the outgoing call.
- 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 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 anyways.