CANADIAN ANTI-FRAUD CENTRE BULLETIN

Bank Investigator – New Variation 2024-08-23

FRAUD: RECOGNIZE, REJECT, REPORT

The Canadian Anti-Fraud Centre would like to warn Canadians about a new variation of the bank investigator scam. Fraudsters are impersonating financial institutions and are claiming that the victim's bank account has been compromised.

Fraudsters will convince victims that in order to protect their account until a new debit card is issued, the victim must send an Interac e-transfer transaction to their own cellphone number. The suspect will instruct the victim on the steps required to add themselves as a payee and to increase their daily Interac e-transfer limit to $10,000 (note that the maximum amount that a sender may send through the Interac e-transfer network may vary depending on the sender's financial institution. Interac will automatically refuse to complete any payment by a sender above the limit established by the financial institution). The suspect provides the e-transfer question and answer that the victim must use for the transfer. Once the victim sends the Interac e-transfer transaction to their own cellphone number, suspects will ask the victim for a "code" which is the last portion of the Interac e-transfer URL/link received. If the victim provides the URL, suspects will have the ability to deposit the funds into their own account.

In some cases, suspects are able to provide some of the victim's personal information which might include name, date of birth, phone number, address and debit card number to make the call seem legitimate. Additionally, suspects are spoofing financial institution phone numbers or are providing fraudulent call-back phone numbers which impersonate the financial institution.

<u>Other variations of the bank investigator scam:</u>

1.) Victims receive an automated phone call claiming to be their financial institution, law enforcement or, in some cases, Amazon advising that there have been fraudulent transactions in their account. Fraudsters will request access to the victims' computer to continue the "investigation". Victims are then shown a fraudulent transaction on their online bank account. The suspects state that 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".

    In some cases, fraudsters will add the victim as a "payee" with a fraudulent email address and advise that the victim must transfer a large amount of money in order to protect their account. The fraudsters will convince the victim that they have added funds to the victim's account but, in reality, the funds were transferred from their line of credit or savings account.

2.) Suspects may have the victims debit card number and password, but cannot access the victim's account due to multi-factor authentication protection on their account. Suspects then proceed

to contact the victim claiming to be their financial institution and will advise the victim that they must provide a code they receive via text message or email in order to confirm their identity. The code the victim provides is the multi-factor authentication code which gives the suspects full access to their bank account.

Warning Signs – How to Protect Yourself

- Criminals use Call-Spoofing to mislead victims. Do not assume that phone numbers appearing on your call display are accurate.
- 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 bank debit card from a different phone if possible or wait 10 minutes before making the outgoing call.
- Never provide details of links or URL's received via text message or email to fraudsters.
- Don't share codes received via text message or email with anyone. In most cases, these are multi-factor authentication codes that will give fraudsters access to your account.
- Fraudsters will often provide the first 4 to 6 numbers of your debit or credit card. Remember that these numbers are used to identify the card issuer and are known as the Bank Identifier Number (BIN). Most debit and credit card numbers issued by specific financial institutions begin with the same 4 to 6 numbers.
- If your personal information has been compromised in the past through a breach or a phishing message, remember that the information can be used as a tool to make the communication appear legitimate.
- Never provide remote access to your computer.
- 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.
- Enabling Auto-Deposits for Interac e-transfers provides additional layer of security
- 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, you should still report the incident to the CAFC.