Fraud – Identification and Prevention

Sgt Doug Mirau

October 8, 2025

ottawapolice.ca

OTTAWA POLICE SERVICE
SERVICE DE POLICE D'OTTAWA

Working together for a safer community
La sécurité de notre communauté, un travail d'équipe

What is Fraud?

- Criminal offence under the Criminal Code of Canada, section 380.
- Fraud is taking something by using DECEIT.
- The person is often tricked into giving money and/or property.
- Most often the victim will appear willing to give their money and/or information because of deception.

Fraud by Numbers

- Approximately 10,000 incoming Fraud Reports per year at OPS
- Over 7,000 are finalized as Fraud
- UCR/CCJS statistics
- CAFC in 2024:
  - 51616 reports
  - $648M
  - Believed to be 5 to 10%

Fraudsters Goal

-Money

-Banking information (C.C. #'s, account #'s, passwords)

-Property (Kijiji/FBM items for sale)

-Personal Info/Identity (Name, SIN#, DOB, Address)

-Gift Cards

Methods of conducting fraud

- Computer/Internet
- Phone
- Door to Door

Counterfeit Cash

- 100's, 50's, 20's currently on the rise being distributed and uttered.
- Examine bills, feel for an edge on the transparency window.
- Look for "prop" in the window.
- Will often have same serial number.
- Use caution when making cash transactions with people you don't know.

Fraud Scams

- Bank Investigator
- Phishing Scams (Banking information)
- CRA Tax Scam
- Smishing Scams
- Renovation/Construction Scam
- Grandparent Scams
- Kijiji/FB Marketplace Scam
- Sim Swap
- Romance Scams/Lottery Scams
- Identity Theft/purchases with info

Computer/Internet Frauds

- *Phishing scams* are perpetrated by cloning, copying and masking the identities of often real email addresses, email documents, websites, messages, etc.
- This is often done by a method known as spoofing.
- Objective to Internet based frauds are to obtain your personal information, banking information, password information and GET YOUR $$$

From: Scotiabank <#Scotiabank-unauthrorized-transfer-cancel-dasdasate-custom.6458334820.no_reply@forum.xda-developers.com>
Date: February 16, 2017 at 7:11:45 PM EST
To: <[redacted]
Subject: Unauthorized TRANSAFER from your Account[6458334820rlp]

Scotiabank

Hello [redacted]

Someone tried to access your Scotiabank account from a new device on 16-Feb-2017.

IP address: 213.64.64.64

Location: Canada 15

The attempt was not successful. Due to this we had to block your account access.

Your account access is now limited and your funds are frozen.

To unfreeze your funds and activate your account access simply follow the link below:

http://www6.scotiabank.com/cgi-bin/rbcgi6r64#attention-notice-pl-6

Computer/Internet Fraud Continued

- CRA Refund Scam

  -Email from CRA indicating that you have a tax refund, (mail.electrnic@payments.interac.ca).

  -Link leads you to a page that indicates you have a $458.00 refund from CRA (amount may vary). Click on a 2nd link.“Deposit to your financial institution”

  -3rd page appears requesting your S.I.N. #, First and Last Name, D.L. #, address, D.O.B., and credit card information.

  *CRA does not send these emails to people or provide refunds via credit cards, gift cards, Amazon cards, etc.

Computer/Internet Frauds Continued

Kijiji and Facebook Marketplace Fraud

-Overpayment with a fraudulent commercial, personal or bank draft of an item being sold.

-Request of the difference being returned, prior to the cheque being cleared as Fraudulent/Fake by the banks.

-e-transfer “link” that looks legitimate but requires you enter banking information, password, etc.

-immediately transfer money from account(s)

Computer/Internet Fraud Continued

- Romance Scam

  -Perpetrated via computer, creating anonymity for the fraudster.

  -Preying on peoples feelings and emotions, making them feel loved and cared for, often in time of need.

  -In time, requests for money for business ventures, for a plane ticket, customs border issues and on and on.

  -Often they use the persona of a high ranking military officer, attractive male or female.

  -Most often the victim has never met the party in person and at most have spoken over the phone.

Phone Frauds

- Bank Investigator:
  - Call from “bank investigator” that card(s) have been compromised/fraud/involved in ot
  - Victim will be convinced that accounts need to be protected and that the bank will pick up “compromised cards” along with passwords and new ones will be issued
  - Account information is changed ie. daily max, contact numbers, etc.
  - Accounts are then drained

Phone Frauds

- Microsoft Scam/Geek Squad

  -Call from “Microsoft Technician” requesting remote access to your computer, because you have a virus on your computer.

  -Malware/spyware commonly installed remotely into your computer to gather personal information from your computer and/or banking information.

  -Also will ask you for your credit card # and they will charge you for their services. It is important to have your computer serviced if contacted by a fraudster

Phone Frauds Continued

- Canada Revenue Agency Scam

  -Fraudulent Phone Calls indicating that you owe back tax money.

  -Requesting you have amounts owing or back taxes with a Credit Card or Gift Card.

  -Will threaten arrest of you and your family

No Government agency will ever request payment via cryptocurrency or gift cards*

Phone Frauds Continued

- Grandparent Scam:

  -Phone call from a caller that identifies as your grandson or granddaughter in need of help because of a car accident, arrest, bail, lawyer fees and generally occurring in another country.

  -They will request that the call be confidential.

  -Request is for you to send money via western union.

  -The requests for money will not stop until you Stop Sending Money!!!!

Phone Frauds Cont.

- Cruise Scam

  -Receiving a phone call/text message that you won a cruise or vacation, and all you have to do is pay the taxes.

- Credit Card Scam

  -Receiving a phone call indicating that your credit card has been compromised and they require you to confirm your card information. Sometimes arrangements are made to pick up cards/then maxed very quickly

Phone

- Lottery Scam

  -Receiving a phone call indicating that you have won a Lottery.

  -In order to collect the winnings you are required to pay the taxes and/or fees to be released from customs or border services.

  -If you didn't play a lottery, you didn't win a lottery, especially in the U.S. or overseas.

Door to Door Frauds

- Charity Scam

  Fraudsters using the cover of legitimate charities to collect money at your door.

  -They will often have a fraudulent badge or I.D. card.

  -High pressure sales tactics.

  -Preying on the holidays or your willingness to give to particular charities (Cancer society, Heart Institute).

  *You can always say No! Contact the charity of your choice and donate directly to them.

Door to Door Frauds Continued

- Renovation/Construction Scam

  -Knock on the door to tell you they just happen to be doing some work in the area and can give you a “special price/group pricing”.

  -Demand a large down payment "to buy materials". Most reputable contractors can maintain charge accounts with their suppliers.

  -Be aware of door to door sales.

  *Be cautious, do your research!!!

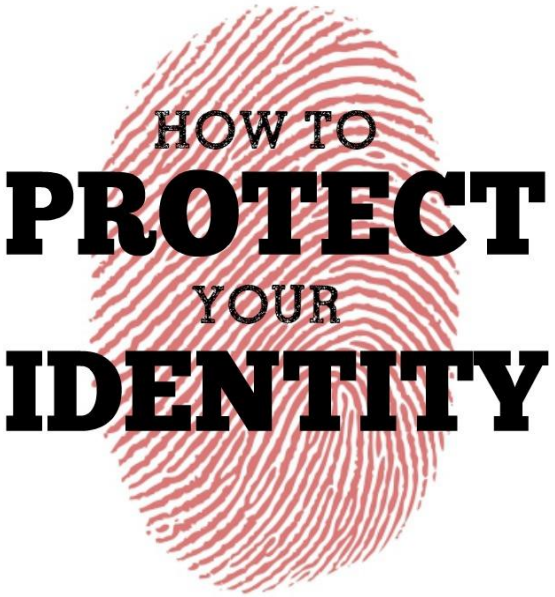
Identity Theft

How your identity is compromised:

- All of the fraudulent scams mentioned above.
- Removing your e-mail or fraudulently redirecting your e-mail
- Stealing from wallets, purses, mail, vehicle, computer, and websites you've visited or e-mails you've sent
- Phone calls, posing as a creditor and bankers
- Information being purchased from a dishonest employee working where personal and/or financial information is stored (banks/telcos, etc.)

Protecting Your Identity

- Burn or shred personal financial information such as statements, credit card offers, receipts, insurance forms, etc.
- Check your personal credit with equifax and transunion periodically and confirm your credit is YOURS!!!
- Victims of Identity theft, flag your credit bureaus
- Put an alert and notifications on your credit cards
- Be cautious when filling out ballots for prizes. Where does that information go?



Credit Bureau

- Equifax Canada

  1-800-465-7166 between 8:00am and 5:00pm ET

- TransUnion

  For residents outside Quebec 1-800-663-9980 between 8:00am and 8:00pm ET

Don’t Ignore the Red Flags

- Sending money internationally. Transferring Money-Western Union, Money Mart, Money Gram, GMT, etc.
- Winning a lottery, cruise or items, without playing
- Having to pay taxes or receiving refunds via credit cards/G.C.
- Paying with gift cards
- Receiving commercial/international cheques as payment

How to Report Fraud?

Non-Emergency Frauds

613-236-1222

(follow the prompts)

Or

Go to Online reporting

Ottawapolice.ca

-Click Online Reporting

-Click Fraud Complaints

Emergency Fraud in Progress-

Prevention

- Passwords – complex, hidden, pw generator
- Avoid certain websites and fake/dummy sites
- Be aware of the use of the word “kindly” as well as emails/messages that are too nice
- Power of Attorney (elderly/vulnerable)
- Talk with friends/family
- If it seems too good to be true, it is
- ROI over 10% is likely fraud
- Use of AI to clone voice – ie. “yes”

Prevention Continued

- Cryptocurrency and AI – use caution
- Counterfeit cash - $100, $50, $20 “prop” money
- Never buy anything on the street/door to door/parking lots – buyer beware
- Consider keeping cards “locked” while not in use
- Keep low profile online and in social media
- Kijiji/FB Marketplace – cash only
- Beware of etransfers from unknown persons

Just say NO

- Don’t be afraid to say no, decline, hangup, etc.
- Be very cautious of incoming calls/messages/emails/ pop-up messages

Questions?