# FRAUD PREVENTION

LETHBRIDGE POLICE SERVICE - PRESENTATION HIGHLIGHTS

## WHAT DO SCAMMERS WANT?

- Your money
- Your personal information; to sell or use to open fraudulent accounts

## REMEMBER THE 3 Rs...

### Recognize

You don't have to be 100% sure it's a scam. Treat every online interaction with caution. Verify before sending money or information.

### Reject

Say "NO!" Stop! Delete! Disengage from further contact.

You do not have to share your money or information with a stranger who claims to be trustworthy.

### Report

Talk to someone you trust who can help guide you.

Suffered a loss? Report to police and your financial institution.

NOT suffered a loss? Report to the Canadian Anti-Fraud Centre.

## GENERAL TIPS FOR COMMON SCAMS:

- **Don't be afraid to say NO!**
  Hang up the call or delete the message.
- **Protect your information**
  Don't give information (or money) to anyone you haven't confirmed is legitimate.
- **Verify the information**
  Never assume the caller ID, email address or website provided are legitimate.
- **Slow down! Do your research!**
  Take your time to evaluate the communication and directions you received. Do your research before responding to anything online.
- **Protect your computer**
  Have your computer inspected by a local professional. Install software to protect your computer. Never allow remote access unless you are absolutely sure you can trust the technician.
- **Don't click!**
  Never click on links you don't trust.
- **Use the security features**
  Use all the security features your financial institution offers.
- **Check your credit**
  Routinely check your credit with Equifax and TransUnion.

## RESOURCES AND CONTACTS:

**Lethbridge Police Service**
403-328-4444 (Non-Emergency)
lethbridgepolice.ca

**Canadian Securities Administrators**
securities-administrators.ca

**Canadian Anti-Fraud Centre**
1-888-495-8501
antifraudcentre-centreantifraude.ca

**Equifax**
1-800-465-7166
equifax.ca/personal

**TransUnion**
1-800-663-9980
transunion.ca

# COMMON ONLINE SCAMS IN LETHBRIDGE

## Phishing Scam

Scammers use technology to send random emails, texts, phone calls or pop-ups, hoping that someone will respond so they can convince them to send money. They often pretend to be a credible business or government agency.

**PROTECT YOURSELF:**

Always verify who you are communicating with.

## Grandparent Scam

Scammers pretend to be a grandchild in trouble and needing money. They will demand that victims withdraw large sums of cash and then arrange to have funds turned over to a "courier."

**PROTECT YOURSELF:**

Confirm with the grandchild, or someone close to them, that help is actually needed. Consider creating a code word that grandparents and grandchildren can use if there is a real emergency.

## Government or Business Scam

Victims are told they owe for fees, taxes or fines, and that there will be legal consequences if they don't pay. Scammers may ask victims to "verify" personal information, which will later be used to open fraudulent accounts.

**PROTECT YOURSELF:**

Get the official phone number of the business/government agency (not the number the scammer gives you) and contact them to verify the claim.

## Computer Fixing Scam

Victims receive a pop-up or phone call from someone claiming to be "tech support." They tell the victim they can fix their computer for an upfront fee.

**PROTECT YOURSELF:**

Never give remote access. Use a reputable local business to fix your computer.

## Lottery Scam

Scammers tell victims they have won a lottery and must pay fees or taxes to collect the prize. Canadians do not pay fees or taxes on lottery winnings.

**PROTECT YOURSELF:**

You can't win if you didn't enter. If you did enter, verify that your ticket matches what the caller is telling you.

## Extortion Scam

Scammers access compromising photos or videos of victims and then threaten to broadly share, unless paid.

**PROTECT YOURSELF:**

Never share compromising images. Never pay the scammer to destroy the images - you have no control of where they are stored or sent.

## Romance Scam

Scammers troll legitimate dating sites to identify victims. They gain the victim's trust and then seek opportunities to ask for money.

**PROTECT YOURSELF:**

Never send money to someone you have never met.

## Investment Scam

Scammers convince victims to invest in an investment that does not exist.

**PROTECT YOURSELF:**

Always do your research. Never invest with a firm that is not registered on the Canadian Securities Administrators website.

## Recovery Scam

Scammers re-contact victims and claim they can recover their losses for a fee.

**PROTECT YOURSELF:**

The only way scammers know you had funds stolen is because they were part of the original scam. Do not pay someone to recover stolen funds.

## Online Market Scam

Scammers take advantage of people buying, selling or renting items online; often using fake payment or shipping scams, or trying to get victims to click on fraudulent links or share their personal information.

**PROTECT YOURSELF:**

Never click on links and verify the money is in your account before releasing an item.

## Money Mule Scam

Scammers ask victims to receive money from someone they don't know and send it to someone else. The victims are actually helping launder stolen money.

**PROTECT YOURSELF:**

Never receive money from, or send money to, someone you don't know without first verifying with a trusted and known source.


## Artificial Intelligence

AI is increasingly used to make scams more convincing and efficient. It also helps fraudsters analyze data to target potential victims.

**PROTECT YOURSELF:**

Be aware. AI can make scams seem VERY convincing (i.e. copy a loved one's voice or appear to be from a real company).