TOPICS

- Current scams and fraud trends
- Prevention tips
- What to do if you are scammed
GOVERNMENT AGENCY SCAM

- Phone call
  - CRA, Immigration, Service Canada, Police
  - Can “spoof” the # to make the call look legit

- Use scare tactics/threats to make you think you’ve done something wrong or someone you love is in trouble (under arrest)
The scam continues...

- You need to pay to get out of trouble
  - Told to pay by way of gift cards (Google Play, Itunes, Steam), credit card #, virtual currency (Bitcoins)

- Demands for personal information
Immigration Scam Video

- https://youtu.be/mNnDz-W3VuI
DATING SCAMS

- Dating Sites: Tinder, Match, Plenty of Fish, Facebook, WeChat

- The person asks for photos, personal information or money
Dating Scam Prevention

- Do NOT send photos

- Do NOT give out your personal information (bank account numbers, credit card numbers or passport numbers)

- Do NOT send money to anyone you meet on-line, regardless of the reason they give
EMAIL FRAUD

- Email from CRA, bank, Paypal, Amazon, etc

- Asked to verify your personal information or advising you there is an issue with your account

- Directs you to use link provided to log in or access website
Confirmation is required

We have received your tax calculation and we have determined that you are eligible to receive a tax refund of 214.178.

To confirm that you want your tax to be refunded, please go to tax refund for individuals and submit the form.

Note: A refund can be delayed for a variety of reasons. For example, submitting invalid records or applying after deadline.

Personal information is collected under the Income Tax Act to administer tax, benefits, and related programs. It may also be used for any purpose related to the administration or enforcement of the Act such as audit, compliance and the payment of debts owed to the Crown. Failure to provide this information may result in interest payable, penalties or other actions. Under the Privacy Act, individuals have the right to access their personal information and request correction if there are errors or omissions.

Please do not reply to this message. It is for your information only.
Email Fraud Prevention

- DO NOT click on any link
- DO NOT provide personal information
- DO NOT log into your account
- Delete the email
COMPUTER SCAMS

- Phone call or email from Microsoft or Apple advising there is a problem with your computer
  - Virus
  - Outdated software, etc

- They ask for remote access to your computer to remove the virus or update your system
Computer Scam Prevention

- Hang up or delete the email
- Don’t give anyone remote access
- Take your computer to a reputable store and have them examine it
- Use a firewall or internet security software to prevent hackers from accessing your data, and keep it updated
- Only use secure sites such as those using “https” and have a closed padlock symbol
E-TRANSFER FRAUD

What is it?

When an email account is hacked and incoming e-transfers are redirected to another email account.
Preventing E-Transfer Fraud

- Ensure the recipient knows when it is coming & send the notify via both email and text message.
- Use a STRONG security question/answer that complies with bank requirements.
- Personally tell the recipient the security answer...NEVER send it as an email/text.
Important...

*Banks will NOT reimburse you if you do not follow their guidelines for sending e-transfers*
CREDIT or DEBIT CARD FRAUD

- Suspect watches you enter your PIN then steals your card (Distraction Technique)

- Cards left in vehicles which are broken into

- Friend/Family Member - You provide them with your card and PIN to make purchases for you
Prevention Tips

- Keep your wallet and purse secure at all times. Never leave them in your car!

- Protect your PIN number. Keep cards in wallet until ready to pay.
More Thoughts...

- Check your statements regularly and report suspicious activity to your bank.

- Notify your bank and police immediately if your cards are lost or stolen.

* If you give out your PIN, the bank will not cover you for fraudulent charges *
RENTAL FRAUD

- Posted online...Craigslist, Kijiji, etc
- Can’t see the place in person
- But you agree to rent
- Demand for deposit and rent $ before getting the home
- Never hear from them again
Rental Fraud Prevention

- Make sure the person showing the home is the landlord or property manager.

- Give minimal personal information, so that you are not the victim of Identity Theft (i.e.: provide your age instead of your birth date).

- Do not wire or pay any money before seeing the home in person.

- Understand your rights as a tenant (Residential Tenancy Act).
If you are scammed:

- Stop ALL contact with the bad guy.

- Keep all your transaction records.

- Report it to your bank IMMEDIATELY.
  - They may be able to stop or reverse a transaction if caught in time.
What to do continued...

- Report it to the police
- Change Passwords, PIN, usernames, etc
- Report it to your passport office/Consulate if you think your ID was stolen
IF IT SOUNDS TOO GOOD TO BE TRUE...

IF YOU ARE THREATENED...

IF THEY ASK TOO MANY PERSONAL QUESTIONS...

IF THEY FALL IN LOVE TOO QUICKLY...
IT'S A SCAM!