ONLINE FRAUDS AND SCAMS

Fraudsters Targeting Older Adults Online
Agenda

1. Introduction to speakers – Kevin Smith and Steve Wilson
2. Older Adults and the Internet
3. Common Internet Frauds and Scams
4. Ways to Beat Frauds and Scams
5. Ways to Prevent Identity Theft
6. Resources, Reporting and Remedies
Your Presenters

Kevin Smith

- Staff Lawyer – BC Centre for Elder Advocacy and Support
- BCCEAS Outreach Program – Frauds and Scams presentations

Cst. Steve Wilson - CFE, CFCl, CCE, CAMS

- Economic/Technical Crime Unit, Delta Police Department
- Fraud Awareness and Prevention Outreach Program
BCCEAS Services

1. **Seniors Abuse and Information Line**
   - 604-437-1940/1-866-437-1940
   - 8am-8pm 7 days/wk

2. **Victim Services**
   - Information, Safety Assessments
   - Support and referrals to victims of abuse

3. **Legal Services**
   - Legal Advocate – housing/benefits/debt
   - Lawyers – elder abuse/guardianship & capacity/residential care

4. **Outreach**
   - Presentations – financial literacy/frauds and scams
   - Website/resources/media/public events
Internet Use in Canada

- Canadians are the world’s biggest Internet users.
- We log an average of 43.5 hours of online browsing per month
- This is almost twice the global average.
Survey on What Seniors Want

Tech-Savvy Seniors in Canada Seeking Digital Capabilities

Internet use tripled among those 65 and older in Canada over the past decade, according to Revera’s 2013 report.

3 in 5 Seniors want digital options to manage their health remotely.

What’s important to seniors?

- 75% Online Access to Health Records
- 65% Online Appointment Scheduling
- 58% Electronic Reminders
- 46% Email Providers

Accenture Health Consumer Survey, 2013
More seniors are using the Internet every day – but their slower speed of adoption makes them easier targets.

Their unfamiliarity with the less visible aspects of browsing (e.g. firewalls, security certificates, built-in ‘add-ons’ and ‘virus’ protection) make seniors especially susceptible to scam emails and traps.

Seniors as a group are also more trusting of others – and may have diminished capacity or impaired executive functioning.
Main Purposes – Online Scams

There are three main goals for online scammers or fraudsters:

- Have you send them money
- Obtain your personal identification information to steal your identity
- Hack your computer so it can be part of a ‘pharming’ operation
Many of us have received an email from a “Nigerian Prince” looking for a partner to help claim an inheritance, or from a British lottery official. These are now getting more sophisticated – with emails that are:
- dressed up with logos,
- realistic looking backgrounds, and
- ‘return’ email addresses that look almost legitimate.
The CRA has identified a number of fraudulent communications requesting personal info:

- Emails
- Text Messages
- Online Forms

Often this will be for an e-transfer of funds (which CRA never does)
Canadian Security Intelligence Services Scam

- One scam is nervy enough to pretend to be CSIS
- You are informed your computer has porn, and that spam messages with ‘terrorist motives’ were sent from your computer
- You have to pay $100 in ‘Ukash’ to have your computer ‘unlocked’
Lottery Proceeds Scam

- Scammers claim to have won the lottery but to have no bank account in which to deposit the winnings.
- Promises the victim a premium in exchange for use of his or her account.
- After the victim makes a “good faith” payment to the offender, the victim never hears from the offender again.
Reverse Mortgage Scams

- The reverse mortgage scam has mushroomed in recent years (1300% between 1999 and 2008) in the US.
- Legitimate reverse mortgages are also increasing in frequency - scammers are taking advantage of this new popularity.
- Unsecured reverse mortgages can lead property owners to lose their homes when the perpetrators offer money or a free house somewhere else in exchange for the title to the property.
Auction Frauds

- A significant proportion of Internet auction fraud involves the non-receipt of an item that has been paid for.
- The victim bids for an item through an Internet auction site and is subsequently notified that he/she is the successful bidder.
- Payment is made to the seller but the merchandise is never sent to the victim. In many cases, the seller defrauds a number of bidders at the same time.
Online Dating

The anonymity of the internet makes it a perfect place for con artists to hide their real intentions while trying to entrap their victims under the guise of romantic interest.
Investment Scams

- Scammers persuade older adults to invest in precious gems, real estate, annuities, or stocks and bonds by promising unrealistically high rates of return – “risk free”.

- The investments often consist of fake gemstones, uninhabitable property, or shares in a non-existent or unprofitable company.

- Pyramid schemes – like Bernie Madoff’s – may also be used.
Travel Packages

- Older adults have more leisure time and so are attracted to low-cost travel packages.

- Many of these packages:
  - cost far more than market rates,
  - provide substandard accommodations, or
  - do not provide the promised services.

Friesen Conference - Online Frauds and Scams
May 15, 2015
Counterfeit Prescription Drugs

- Most commonly, counterfeit drug scams operate on the Internet, where seniors increasingly go to find better prices on specialized medications.
- The danger is that besides paying money for something that will not help a person’s medical condition, victims may purchase unsafe substances that can inflict even more harm.
- This scam can be as hard on the body as it is on the wallet.

**COUNTERFEIT DRUGS CAN KILL**
(or seriously mess up your life)

Can you really tell the difference between a phony drug & the real thing? Clever counterfeiters can fool you.

**WHY THIS IS SO IMPORTANT:**

Counterfeit drugs...
- May have been manufactured in unregulated third-world factories
- May contain little or none of the active ingredient in the real thing
- May have unlisted, harmful additives
- May contain toxins that can undermine your health or even kill you
- Are illegal and subject to seizure (which could result in serious legal problems for YOU)

It’s just not worth the risk.

AccessRX.com
Fake Charities

- Money is often solicited for fake charities after natural disasters.
- People also feel especially kind-hearted and generous during the holiday season – scammers ramp up during this time.
If It Seems Too Good to Be True...

Have you ever wondered how ads such as this can appear on Facebook?

Does anyone really believe that you can buy an iPad for 90% off the price of even an iPad model 1?
What makes the email *seem* real?
What looks ‘phishy?’
Going Phishing

From: Royal Bank of Canada [securityclient@rbc.com]
Sent: 2012, July, 20 7:33 PM
To: undisclosed-recipients
Subject: Account ALERT - Your RBC Account is at Risk!

Dear Client

Royal Bank Financial Group audit department has detected a problem with transactions in your account. An amount was deposited and withdrawn by our accounting system. We warn you of this error so that you are not surprised when you see these transactions on your monthly statement. No Transaction expenses occurred. Never reveal your personal information on a site other than the RBC secure site. If you noticed another error, contact your institution during opening hours.

We encourage you to **immediately** connect to your account and verify your transactions, by clicking the secured url below:

https://www1.royalbank.com/cgi-bin/rbaccess/

https://www1.royalbank.com/cgi-bin/rbaccess/

http://royalebanking.lv6.com/login.html

RBC Financial Group

- What makes the email seem real?
- What looks suspicious?
Variations on Phishing

- **Spear Phishing** – ‘friending’ someone using a social site (Facebook, MySpace) - a message is then left in an inbox containing questions or links to other sites; or malicious code embedded in a web link that prompts users for information.

- **Pharming** – a fake website - changing the IP address of the target (bank) web site from its real IP address to the IP address of the fake website – with a fake SSL certificate as well!

- **Vishing (voice phishing)** & **Spoofing** – email getting people to call a phone # - connected to a Voice over Internet Protocol (VoIP) phone that can recognize, and record, telephone keystrokes - computer-generated voice instructs callers to enter their credit card number, expiration date and verification code.
Pop Up Virus Warnings

Pop-up browser windows simulating virus-scanning software will fool victims into either:

- downloading a fake anti-virus program (at a substantial cost) OR
- Downloading an actual virus that will open up whatever information is on the user’s computer to scammers.
‘Microsoft Tech Support’ Calls

- Someone may call you on the telephone and claim to be from Microsoft, or “Microsoft Operating System.”
- They might offer to help solve your computer problems – and ask you to follow their instructions to access your computer.
- They might try to sell you a software license.
Ways to Beat Frauds and Scams

- If it looks or sounds too good to be true, it probably is.
- Don’t sign up or agree to ‘special’ offers or deals readily.
- Don’t provide your personal and/or financial info. to others, until you have verified their credentials and reputation.
- Seek independent advice from people or organizations you trust, if an offer involves your money, personal information, time or commitment.
Fraudster Fighter Tool Kit

Get The Guides:
- How to be an Informed Investor
- The Private Placement Market for Retail Investors

Download The App
- REPORT FRAUD
- BeFraidAware

Printable Info Sheets
- Fraud Warning Signs
- Fraud Among Friends
- Identify Con Artists
- Report Investment Fraud

Subscribe
Check out InvestRight.org Community page

Videos: How Fraudsters Work
Watch Now
An Identify Thief Can…

- Apply for credit cards or loans
- Open a bank account
- Write bad cheques
- Acquire new government documents
- Sell or mortgage your house

See Office of Privacy Commissioner, Factsheets, Identity Theft, online: <http://www.priv.gc.ca/fs-fi/index_e.cfm>
Ways to Prevent Online Identity Theft

- Always ensure the site has a valid secure certificate [https://].
- Watch out for ‘self-signed’ certificates.
- Don’t add “exceptions” unless you know what you’re doing.
- Sign out or log off after accessing websites with your personal or financial information – to purge info.
Welcome to the New Canadian Identity Theft Support Centre
Seniors ID Theft Protection Guide

- The Canadian Identity Theft Support Centre has created a guide for seniors on protecting identity from theft.
- It helps them understand the problem and how to protect themselves.
- They also product a Victim Toolkit – how to respond to an ID theft.
Setting up ‘no cookies’ or using “private browsing” so no ‘cookies,’ isn’t foolproof. Other types of tracking technologies can still remain stored during these ‘private’ sessions. In order to clear all the different forms of tracking technologies, you generally have to install and use special tools in your browser. You can also visit the [http://donottrack.us](http://donottrack.us) website for more information on how you can prevent tracking.
What Can Be Done for Victims of Frauds & Scams

- Call Seniors Abuse & Information Line or Lawyer Referral Service
- Find out if there is a legal solution
  - OR
- File an official complaint with BBB or Office of Privacy Commissioner
Reporting Frauds & Scams

- File a report by contacting:
  - Your local police force (NOT 911)
  - Your bank/financial institution and credit card company
  - InvestRight BC
  - Canadian Anti-Fraud Centre

- Call the national credit bureaus to place a fraud alert on your credit reports:
  - Equifax Canada  1-800-465-7166
  - TransUnion Canada  1-877-525-3823
Civil Law

- Take the business or individual(s) to Small Claims Court
- Try to get money back
- Can be difficult – may be nothing left
- May be difficult to track down fraudster/scammer

**First step: Get legal advice!**
Possible related charges:

- Theft
- Forgery
- Extortion
- Fraud

**First step:** Contact the police or the Canadian Anti-Fraud Centre.
The End

Questions?