1281 W Georgia St #310 1-866-437-1940
Vancouver, BC. V6E 3J7 info@seniorsfirstbc.ca

 Revised June, 2026

Land Acknowledgment

We acknowledge that Seniors First BC's head office is located on the traditional, unceded and ancestral territories of the
xʷməθkʷəy̓əm (Musqueam),
Sḵwx̱wú7mesh (Squamish), and səlilwətaɬ
(Tsleil-Waututh)
Nations.

Seniors First BC operates throughout British
Columbia, which spans the traditional and ancestral territories of over 200 First Nations.
We thank them for stewarding these lands and

waters since time immemorial.

Seniors First BC serves all seniors in BC
and engages in dedicated outreach to Indigenous Elders.

Overview of Seniors First BC

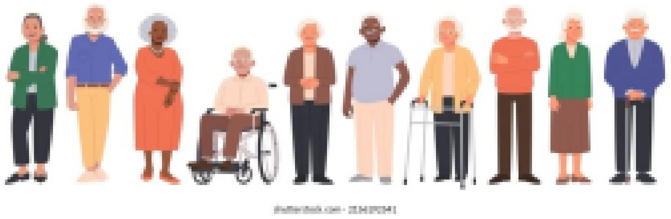
A non-profit charitable organization, providing information, advocacy, and support for older adults across BC with issues affecting their well-being.

- Seniors Abuse and Information Line (**SAIL**)
- Victim Services

- Public Education and Outreach
- Legal Services

  www.seniorsfirstbc.ca

Come visit our info table!



Seniors Abuse and Information Line (SAIL)

- *A confidential information & referral helpline*

- *A safe place to speak about concerns of abuse or neglect*
- *The entry point to access Seniors First BC services*

604-437-1940 or **1-866-437-1940** (toll free)

8am to 8pm weekdays

except holidays

Language interpretation available, including ASL

Email: info@seniorsfirstbc.ca

seniors first BC

Victim Services

Provides the following supports to **older adults 55+** who have been victims of abuse, family and/or sexual violence:

- Safety planning
- Liaison with justice system personnel
- Assistance with Crime Victim Assistance Program applications
- Information and referrals e.g. criminal justice system; community resources

seniors first BC

Public Education and Outreach

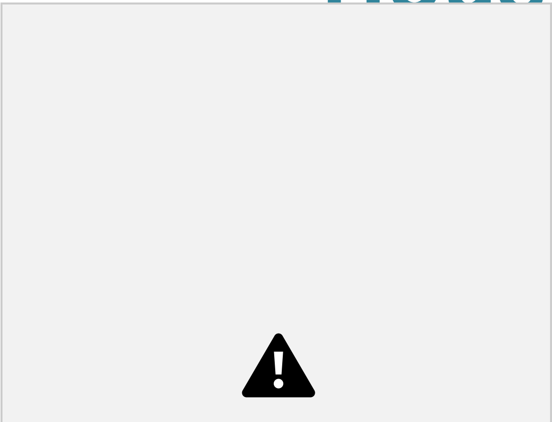
Raise awareness about key issues affecting older adults

through:

Presentations & Events
Publications, Newsletter

Website

Navigating Home Care & Senior Housing: An Advocacy Guide



- Information about:
  - supports in the community
  - entering, living in, and leaving assisted living and long-term care
  - rights and resolving problems

- resources

Access online at:
www.seniorsfirstbc.ca/resources/publications

7

Legal Services

Free legal services for **eligible** older adults with **select** legal issues through: Elder Law Clinics, Legal Advocacy Program, and Advance Planning Clinics

Housing
(Residential tenancy, assisted living, long term care)

Debt

Gov. benefits
(Federal e.g. OAS/GIS
Provincial e.g. SAFER)

Financial exploitation

Family law

Guardianship

Age discrimination

Draft legal documents
e.g. Wills, POAs, Representation Agreements

Other elder abuse

Criminal

la

w

Legal Services Eligibility Criteria

- **Age:** 55+ (50+ for Indigenous Elders, First Nations)
- **Eligibility based on income & all assets**

  Income ceiling (gross): $45,000 for 1 person

  + $20,000 per additional household member

  Assets under $250,000.

- *Eligibility in any case is determined by SFBC lawyers*
- *Exceptions considered on a case-by-case basis*
- Contact the SAIL Line for information and/or to arrange a consultation with the legal team.

Please note the wait time for a callback from the legal team could be up to 4 weeks.

Learning Outline

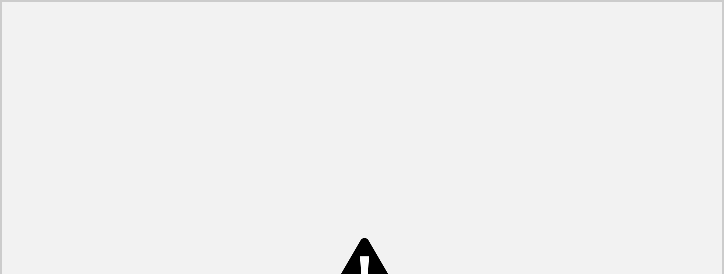
1. What are Frauds and Scams?
2. The Fraudster's Toolbox
3. Common Scams targeting older adults
4. Safety Strategies

5. Resources

Defining Frauds and Scams

- *Fraud is the wrongful or criminal deception intended to result in financial or personal gain*

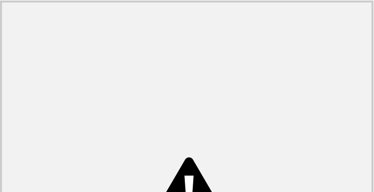
- Frauds and Scams are **crimes**



- The two terms are used interchangeably
- Fraudsters may target victims for a wide variety of reasons

Fraud and Scam Statistics

In 2025*



40,679 reports of fraud processed
27,693 victims of fraud
$704 M lost to fraud

Only 5 to 10% of victims report to the Canadian Anti-Fraud Centre (CAFC) or law enforcement

*Source: Canadian Anti-Fraud Centre

How Are New Scams Created?

- More sophisticated and creative scams by local and international crime organizations

- Based on latest events, trends, or technology:
  - COVID-19 pandemic, wildfire/floods
  - Online banking
  - Cryptocurrency (Bitcoin)
  - Online dating apps and social media
  - Government updates
  - Artificial intelligence (AI)

2. The Fraudster's Toolbox - Same Methods, New Schemes

Countless schemes are created daily,
but the strategies and "tools" remain the same!

- Impersonation
- Urgency

- Emotional Manipulation
- Threats
- Phishing
- Spoofing
- Links
- Pop-Ups

Adopted from Canadian Anti-Fraud Centre's "What's in a Fraudster's Toolbox?"

Impersonation

- Fraudsters impersonate anyone to trick victims into sending money or sensitive information

• Involves lots of planning - scammers may do **"social media mining"** for info about targets

Safety Tip!

• Never trust that a message is from who the sender says they are, especially when including requests • Try to verify their identity using several means • Keep your information online private!

Emotional Manipulation

- Fraudsters take advantage of emotions, such as fear, anxiety/stress, guilt, loneliness, excitement

- Emotions help fraudsters trick victims into believing their story and giving them money

Safety Tip!

- Be suspicious of interactions (online, phone, or in-person) where someone has a sob story, professes love or friendship to you, tells you something exciting, or makes you feel unsafe

Urgency

- Fraudsters use urgency to trick victims into sending money, personal information, or clicking on malicious links

- Urgency pressures victims by giving them less time to consider whether the request is suspicious

Safety Tip!

- Time is on your side!
- Take at least 5 minutes (or longer) to think about whether a call or message

is suspicious

Threats

- Often used alongside urgency and emotional manipulation
- May include threats of arrest, physical harm, financial harm, release of sensitive information or pictures, or harm against family members

Safety Tip:

• Ignore suspicious calls or messages, especially if you are unsure about the legitimacy or asked for money or information

Phishing

• Phishing attacks:

-**fraudulent emails, text messages, phone calls or websites** -trick users into downloading malware, sharing sensitive information or personal data (including **passwords, account details, usernames**) • Can be generic scams OR

a targeted attack focused on a specific individual

Safety Tip!

• **Never click on links or attachments** in emails, messages, ads • Take time to be a detective with every message & phone call • Verify by contacting company directly

• If unsure, get help.

Spoofing – phishing tool

- A digital method to convince victims that they are communicating with people they know, or legitimate companies/organizations
- May include **changing the caller-ID** displayed on phones or the **sender address** in an email, or **mimicking legitimate websites**

Safety Tip!

- Take time to be a detective with every message and call you get!
- If unsure, get help

Spoofing – a phishing

- The fake message isn't always bad news – sometimes the fraudsters want to offer us a prize!

- Example: a fake email/ad pretending to be from CAA/BCAA asks you to do a quick survey and WIN a car emergency kit

Safety Tip!

- If you're interested in the advertised product or contest, contact the company directly to verify. Don't click on ads!

Links

- Fraudsters send out hundreds of thousands of messages with malicious links as they are guaranteed to catch someone who clicks on one
- Malicious links can look suspicious or legitimate

Safety Tip!

- Don’t click links in messages, emails, or social network sites and get a second opinion!
- Remember: the government/CRA, police, ICBC, banks will not send text messages

Digital Pop-ups

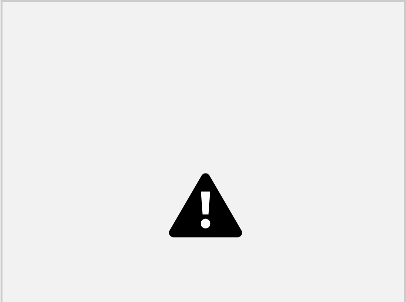
- Boxes that pop up on your computer or device screen that may say you've won a prize or your computer is infected with a virus, malware or spyware

- Clicking on pop-ups may install malicious software or lead you to a fraudulent site

Safety Tip!

- Never call a number in a pop-up ad
- Install anti-virus protection and pop-up blockers

Artificial Intelligence (AI)



- **Voice cloning** – AI is used to imitate someone's voice
- **Deepfake Images/Video –** AI can be used to create images or a video of anyone—a celebrity, a politician, even you! The body moves, the mouth moves, voice is imitated - creates an illusion that the video is real.
- **Emails/text messages/social media messages** –

AI can be used to create messages with few or no typos, and seem legitimate

- **Graphics/logos/websites** - AI can be used to create fake images, advertisements

Safety Tip!

websites,

- *Remember the fraudster's toolbox – emotional manipulation, urgency, threats, requests for money or information!*
- *If it sounds too good to be true, it probably is!*

Examples of Common Scams

26

Grandparent/Emergency Scam

- Fraudsters call and pretend to be a family member in distress or law enforcement claiming that a loved one is in trouble, and needs money immediately

- Fraudster's Tools: urgency, impersonation, spoofing, and emotional manipulation

Safety Tips:

- **End the call,** don't send money (or gift cards), and phone the grandchild/family member to learn what’s really happening

- **Set a verbal codeword** with kids, family members, trusted friends to use in messages asking for help
- **Ask a question that only family member knows the answer to**

Romance Scam

- Scammers gradually develop relationships by preying on feelings of loneliness and isolation
- often use fake online dating sites or social media profiles, messages on social media or "wrong number" texts (e.g. “Are we still on for

lunch?" "What's new?") ○ Try to develop a bond, trust, relationship

- Fraudster's Tools: urgency, spoofing, impersonation, links, emotional manipulation

Red Flags:

  - The person seems perfect and professes feelings quickly;
  - asks for more private method of communication;
  - any attempts to meet in person are cancelled;
  - discourages you to talk about them to friends/family

Investment & Cryptocurrency Scams

- Promises of high returns on investments, often with **deceptive**

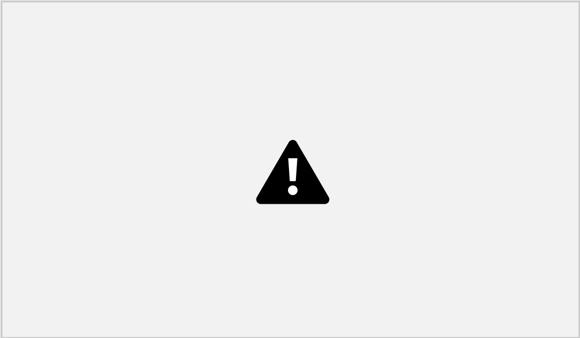
advertising, fake investment platforms, & involving **cryptocurrency**

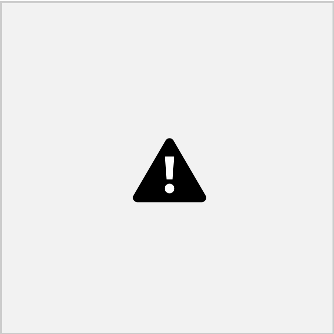
- Fraudster's Tools: Spoofing, links, digital pop ups, emotional manipulation, impersonation, AI-deepfakes

Safety Tips:

- Be wary of individuals, including celebrities or an online connection, or even friends or family, who try to convince you to invest in cryptocurrency
- Be skeptical of promises of large, quick, and low-risk returns
- Do your research and get a second opinion!
- Add a **Trusted Contact Person (TCP)** at your bank/credit union

Cryptocurrency Scams: AI-generated, deep-fake ads/videos

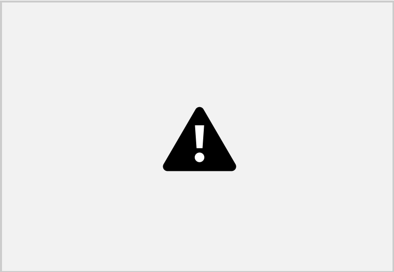




Service Scams

Fraudsters pretend to provide a wide variety of legitimate services.

- **Financial Services – *Bank Investigation Scams***



- **Telecommunication / Utility Service providers**
- **Home Repairs/Services**

  e.g. door-to-door offers for roof repair/gutter cleaning, air duct cleaning, furnace/hot water tank installation

- **Tech Support –** unsolicited calls, want advance fee to fix computer issue •

Marketplace ads -

- Never send a deposit to hold an item, or pay upfront if you haven't seen the item
- Beware of **rental ads, job ads** – too good to be true; asking for deposit or payment in advance

31

Recovery Scams

Don't be conned twice

Fraudsters are **impersonating the Canadian Anti-Fraud Centre (CAFC), law enforcement agency or government department**

- claim they've recovered your lost funds, but you need to **pay an advance fee**
- ask for your help with an ongoing investigation or "sting" operation

Tips:

- Don't be afraid to **hang up** the phone
- **Never pay an advance fee** to obtain a refund
- If you are unsure, contact your local police or the CAFC directly

Online Shopping – Red Flags

- Avoid "sponsored" links especially on social media sites;
- **type the company website into**

your search bar

- Beware **look-alike online shops** – hover over hyperlinks to see URL (website address)
- Urgency in sending money
- Prices drastically reduced/below market rates
- You haven't seen the goods being purchased in person
- **Beware of scammer accounts on marketplace websites (incl Facebook, craigslist, Kijiji, e-Bay)**

Other Scams

- **Distraction scams -** Thieves create a distraction in order to steal valuables; may work alone or with others
  e.g. asking for directions, offering fake jewellery, physical contact like hugs to swap items or steal a wallet/phone, staging a fight or argument

- **Gift Card scams –**
  - Avoid buying gift cards on public kiosks or racks
  - Check for tampering on back of card, especially the sticker for the code
  - Make sure that the cashier hands you the gift card they activated

- **Charity frauds -**
  - Always ask for or locate the charitable tax number and confirm their registration by phone at 1-800-267-2384 or online: Canada Revenue Agency - List of charities.
  - Donate at the source. Don't use links sent by text or email.

- **Fake contests & giveaways –** verify/visit company's website.
  - Don't click links in emails, text messages, or ads

QR Code Safety

QR Codes can be compromised

- Users may be directed to a phishing website which looks legitimate; tricked into entering sensitive info
- Malware may be embedded in the QR code & downloaded into the device

Protect your Device

- **Verify** before scanning (confirm the source)
- Configure phone settings: ask permission & verify before launching the QR code action
- **Avoid scanning QR codes posted in a public setting or on a**

label

- Avoid scanning QR codes received in emails or text messages

https://www.malwarebytes.com/cybersecurity/basics/what-is-a-qr-code
https://www.cyber.gc.ca/en/guidance/security-considerations-qr-codes-itsap00141

l Safety Strategies

What are some ways we can protect ourselves from fraud?

Safety Strategies

• Never accept from or send money to a third party without verifying • **Avoid reacting automatically** – take time, ask questions, listen to instincts • **Verify the caller/message sender** before taking any action • Do not provide personal or financial information on demand

- **Shred papers** with personal information before recycling • Use **voicemail to screen calls** or set up a **call control/call-blocking feature** for your phone
- Remember the **red flags:**
  - Requests for payment using **gift cards, wire transfer or cryptocurrency** (e.g. Bitcoin)
  - Requests for **advance fees** to receive refund, goods, services or a prize
- *If something doesn't seem right, ask someone you trust*

Cyber Hygiene

- **Set strong passwords / passphrases**

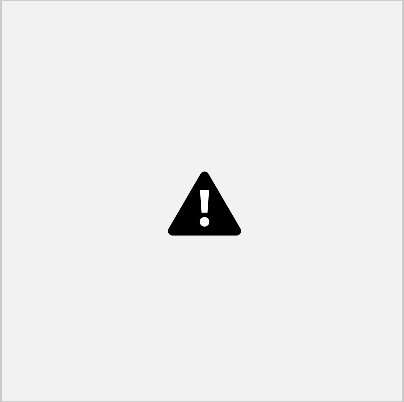
-ideally 16-20+ characters (letters, numbers, symbols)

-passphrase – ideally four or more random words

e.g. sun stone cat chair = Sun$toN3cA#cHa1r

- **Enable 2-step / multi-factor authentication**
- **Avoid using auto-save features for credit card or passwords** • **Don't click on links** from unsolicited messages/emails • Don’t respond to a vague message (e.g. Hi, how’s it going?) • Set social media accounts to "private"
- Verify identities of friend requests
- Be cautious when using public Wifi

Encourage Reporting!



- **Report scams & frauds to the police/RCMP,** or **Canadian Anti-Fraud Centre**
  – this may help with recovery or preventing future damages
- Reporting helps law enforcement address new scams, enact systems changes, and inform the public
- Tell family, friends, other people so they learn from your experience

What to do if you're a victim of fraud

- **Collect your thoughts & gather information**
- **Contact your financial institutions**
- **Contact the police**
- **Report the incident**
- **Protect yourself from future fraud**

From THE CANADIAN ANTI-FRAUD CENTRE

https://antifraudcentre-centreantifraude.ca/scams-fraudes/victim-victime-eng.htm

TransUnion also has information:
https://www.transunion.ca/assistance/fraud-victims-resources

4. Resources

- Local police/RCMP
- Canadian-Anti Fraud

Centre ● Canada Revenue

Agency (CRA) ● Bank/Financial Institutions ● GetCyberSafe.ca

● Cyber-Smart.ca

● Others

Local Law Enforcement

- Contact police/RCMP if you fall victim to a fraud or know someone who has
- They assist with investigations and reports to the Canadian Anti-Fraud Centre (CAFC)

Find a **list of non-emergency numbers** at:
https://www.ecomm911.ca/non-emergency-calls/find-your-local-non emergency-numbers/

Canadian Anti-Fraud Centre (CAFC)

Report a scam, fraud or cybercrime

whether you are the victim, were targeted or are a witness.

Online Fraud Reporting System

https://reportcyberandfraud.canada.ca/

or call (toll-free) **1-888-495-8501** **(Mon-Fri, 8am-4:45pm EST)**

For **updates on scams & fraud alerts**, check CAFC website regularly: https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

Canada Revenue Agency (CRA)

- Latest CRA scam alerts
  - Examples of fraudulent communications
  - What to do if you experience a CRA scam or fraud

Check their website regularly: (search “Canada Revenue Agency scam alerts”)
https://www.canada.ca/en/revenue-agency/corporate/security/protect-yourself-against-fraud/scam alerts.html#h2

If you are unsure and want to confirm if the CRA contacted you, call:
Individuals: 1-800-959-8281 / Businesses: 1-800-959-5525

Banks/Financial Institutions

- Contact your financial institutions/banks about suspicious communications received, including questionable messages about your accounts

- Regularly **review bank / credit card statements**
- Consider setting **limits** on debit/credit card transactions, setting up **transaction notifications**

Credit Bureaus can put fraud alerts on your credit report: Equifax: **1-800-465-7166**
TransUnion: **1-866-525-0262**

Getcybersafe.gc.ca

● a national public awareness campaign ● created to inform Canadians about cyber security and simple steps to protect themselves online
https://www.getcybersafe.gc.ca/en

Fraud Prevention Toolkit for Older Adults

https://cba.ca/Assets/CanadianBankersAssociation/Documents/Articles/Scam_Prevention_Toolkits/2025cybersecurityolderadulttoolkitupdated_en.pdf

-Canadian Bankers Association in partnership with Getcybersafe.ca

Cybersecurity Awareness for Seniors

https://cyber-smart.ca/

Lots of information about different types of scams, along with videos and tips to stay safe.

Other Resources

The Little Black Book of Scams –

https://competition-bureau.canada.ca/en/little-black-book-scams-2nd-edition

People's Law School – *Scams, Identity Theft*

https://www.peopleslawschool.ca/category/consumer/scams-identity-theft/

Get information and technology support; digital literacy sessions

- Local libraries, senior centers, community centers

- **Gluu Society** – www.gluusociety.org

  -free digital literacy skills; apps, social media, Artificial Intelligence
- **Cyber-Seniors** – www.cyberseniors.org

  Book a one-on-one tech call, sign up for a webinar

  Call toll-free 1-844-217-3057

Stay Up-to-Date!

- Inform family members/friends about scams and related resources

- Stay connected safely with others to prevent loneliness and social isolation

- Check the Canadian Anti-Fraud Centre website and other resources

- Watch/listen to the news

We are thankful for the support of:

Phone: 1-866-437-1940
Email: info@seniorsfirstbc.ca