

# Webinar: Online Safety, Security & Scams

Presented by:



**United Way**  
British Columbia

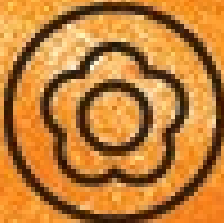
**HelpAge**

**Canada**




December 13, 2023

# Land Acknowledgement





# Agenda

- 1. About HelpAge Canada (10 min)**
  - 2. Introducing this Webinar & Ongoing Support (5 min)**
    - Survey of Needs (20 min)
  - 3. Safety, Security & Scams Presentation (30 min)**
  - 4. CORE Canada, CORE BC & the Tech Resource Library (10 min)**
  - 5. Q&A: Open Session with HAC (Optional) (15 min)**
- 

# About HelpAge Canada







# Helping older persons live with dignity in Canada and around the world since 1975.

Our **vision** is simple: we want to see a world where all older persons lead secure, healthy, active, and dignified lives.

Our **mission** is to support **community-based initiatives** to improve the lives of older persons and their communities.

TOGETHER, WE CAN CREATE A  
NEW NORM WHERE EVERYONE  
CAN AGE WITH DIGNITY!

# WE MAKE CHANGE HAPPEN

To transform the aging landscape, HelpAge Canada has adopted a holistic approach to healthy aging, working to make change in **four impact areas** that encompass the most pressing issues facing older people today:

- **Health and wellness**
- **Aging in place**
- **Digital literacy**
- **Humanitarian relief**

By focusing on overall impact to guide our programs and initiatives, we're doing more than just putting a band-aid on a few issues – we're building stronger communities where older people receive the **support they need** and can **participate fully.**



# Introducing this Webinar & Ongoing Support



# HelpAge Canada & UWBC

HelpAge Canada has been working with the United Way of British Columbia's Healthy Aging team for 3 years, supporting the **Digital Learning** funding stream.



## Support is expanding!

No matter what granting stream you are, webinars and resources will be made available for you!



# HelpAge Canada & UWBC

What has this support looked like in the past?

- Feature Apps
- Tutorials
- Guest Speakers
- Peer Learning
- Webinars
- Resources such as: How-To Guides/ Tutorials, Teaching Best Practices, Research Studies,
- Referrals for funding opportunities, potential partners, equipment & data, etc.

# Survey

**To help us provide the best resources and content to meet your needs, we need your input!**

- **15 min:** Complete Survey

Link to survey shared in the Chat



# Survey

## **Survey Categories:**

- 1) General information about your agency to understand if you are currently offering digital literacy programs/ services and at what level
- 2) Questions about **SKILL** Building needs
- 3) Questions about **TOPICS**/ Information needs
- 4) Questions about **CHALLENGES**
- 5) Questions about **EXPERTS/ PARTNERS** you would like to meet

# Safety, Security & Scams



# Office of the BC Seniors Advocate

**December 7, 2023:**

“Scams are particularly common over the holiday season as fraudsters take advantage of increased activity, stress, distraction and generosity. Many of these attempts are targeted specifically at seniors.”

**Canadians lost more than \$527 million through various scams over the first six months of 2023, according to figures reported to the Canadian Anti-Fraud Centre.”**





According to a new study, 46% of Canadians say they have encountered malicious activity while shopping online. And Christmas is a prime time for scammers to take advantage of online shoppers. So to help educate consumers, here are 12 common criminal scams to be wary of.

# 12 scams of Christmas

## 1 Not-so-merry mobile apps

Official-looking software for holiday shopping could be malicious, designed to steal or send out your personal data.



## 2 Holiday mobile SMS scams

*Fake* Installer tricks Android users into thinking it is a legitimate installer for an application and then quickly takes advantage of the unrestricted access to smartphones, sending SMS messages to premium rate numbers without the user's consent.

## 3 Hot holiday gift scams

Ads that offer deals on must-have items, such as PS4 or Xbox One, might be too good to be true. Clever crooks will post dangerous links, phony contests on social media sites, and send phishing e-mails to entice viewers to reveal personal information or download malware onto their devices.

## 4 Seasonal travel scams

A hotel's Wi-Fi may claim that you need to install software before using it and instead infect your computer with malware if you "agree."



## 5 Dangerous e-seasons greetings

Official-looking software for holiday shopping could be malicious, designed to steal or send out your personal data.



## 6 Deceptive online games

Many sites offering full-version downloads of Grand Theft Auto, for example, are often laden with malware, and integrated social media pages can expose gamers, too.



## 7 Shipping-notification shams

Phony shipping notifications can appear to alert you to an update on your shipment, when in reality, they are scams carrying malware and other harmful software.

## 8 Bogus gift cards

Beware of gift card ads on Facebook and Twitter that claim to offer exclusive deals online.



## 9 Holiday SMiShing

SMiShing is commonly seen in gift card messages, where scammers pose as banks or credit card companies asking you to confirm information for "security purposes." Some even include the first few

## 10 Fake charities

Cyber criminals capitalize on Christmas generosity by setting up fake charity sites and pocketing the donations.



## 11 Romance scams

With so many niche dating sites now available to Internet users, it can be difficult to know exactly who the person is behind the screen. Messages sent from an online friend can include phishing scams, where

## 12 Phony e-tailers

With so many shopping online at Christmas, scammers set up phony e-commerce sites to steal your money and



# Browse Scams – the Canadian Anti-Fraud Centre

## A

[Air duct cleaning](#)  
[Asian community, telephone calls targeting the](#)

## B

[Bank investigator](#)  
[Bomb threat](#)  
[Business executive spoofs and wire fraud](#)  
[Business grants and loans](#)  
[Business opportunity](#)  
[Business proposals, fake](#)

## C

[Canada Revenue Agency](#)  
[Car wrapping](#)  
[Card-not-present](#)  
[Charity](#)  
[Collection agency](#)  
[Continuity](#)  
[Counterfeit merchandise](#)  
[COVID-19](#)  
[Cryptocurrency](#)

## D

[Denial of Service \(DOS\)](#)  
[Distributed Denial of Service \(DDoS\)](#)  
[Donation](#)

## E

[Emergency](#)  
[Explicit video](#)  
[Extortion](#)

## F

[Fake business proposals](#)  
[Fake grant](#)  
[False billing](#)

- [Directory](#)
- [Office supplies](#)

[Financial agent](#)  
[Financial industry client spoof](#)  
[Foreign lottery](#)  
[Foreign money offers](#)  
[Franchise opportunity](#)

## G

[Gem](#)  
[Government documents, help with](#)  
[Grandparent scam](#)  
[Grant](#)

## H

[Head office spoof](#)  
[Hitman](#)  
[Holiday scams and fraud](#)  
[Hostage](#)  
[Hydro](#)

## I

[Identity theft and fraud](#)  
[Immigration extortion](#)  
[Immigration website](#)  
[Inheritance](#)  
[Initial Coin Offerings](#)  
[Investment](#)

## J

[Job](#)  
[Job: counterfeit cheque](#)

## L

[Loan](#)  
[Lottery, foreign](#)  
[Low interest rate offers](#)

## M

[Merchandise](#)  
[Money mule](#)  
[Money offers, foreign](#)  
[Mystery shopper](#)

## P

[Pardon](#)  
[Payroll spoof](#)  
[Personal information](#)  
[Phishing](#)  
[Ponzi](#)  
[Prize](#)  
[Prize winner call](#)  
[Psychic](#)  
[Pump and dump](#)  
[Pyramid](#)

## R

[Ransomware](#)  
[Recovery pitch](#)  
[Resale](#)  
[Romance](#)

## S

[Service](#)  
[Sextortion](#)  
[Sim card swap](#)  
[Spear phishing](#)  
[Subscription trap](#)  
[Supplier/contractor swindle](#)

## T

[Taxpayer](#)  
[Tech support](#)  
[Telephone calls targeting the Asian community](#)  
[Timeshare](#)  
[Timeshare resale](#)

## V

[Vacation](#)  
[Vendor fraud](#)  
[Video, explicit](#)

## W

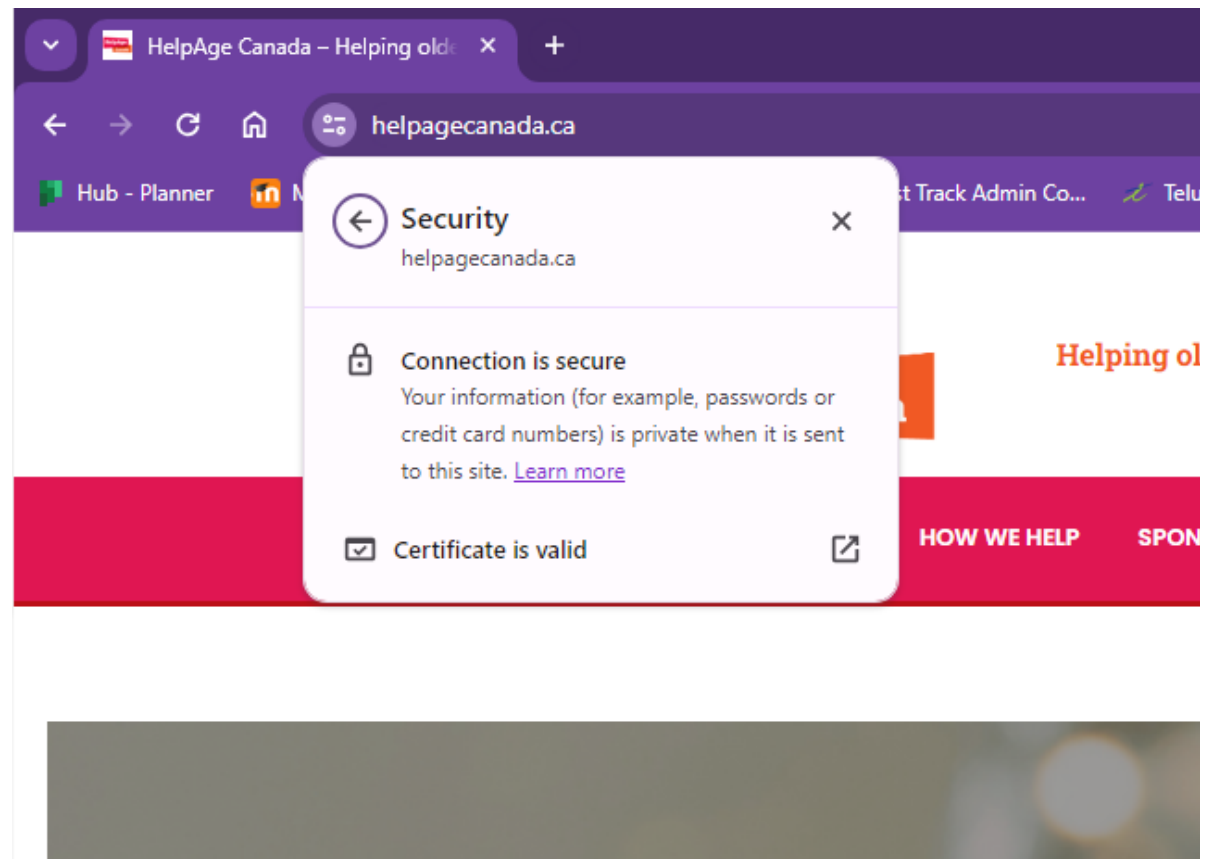
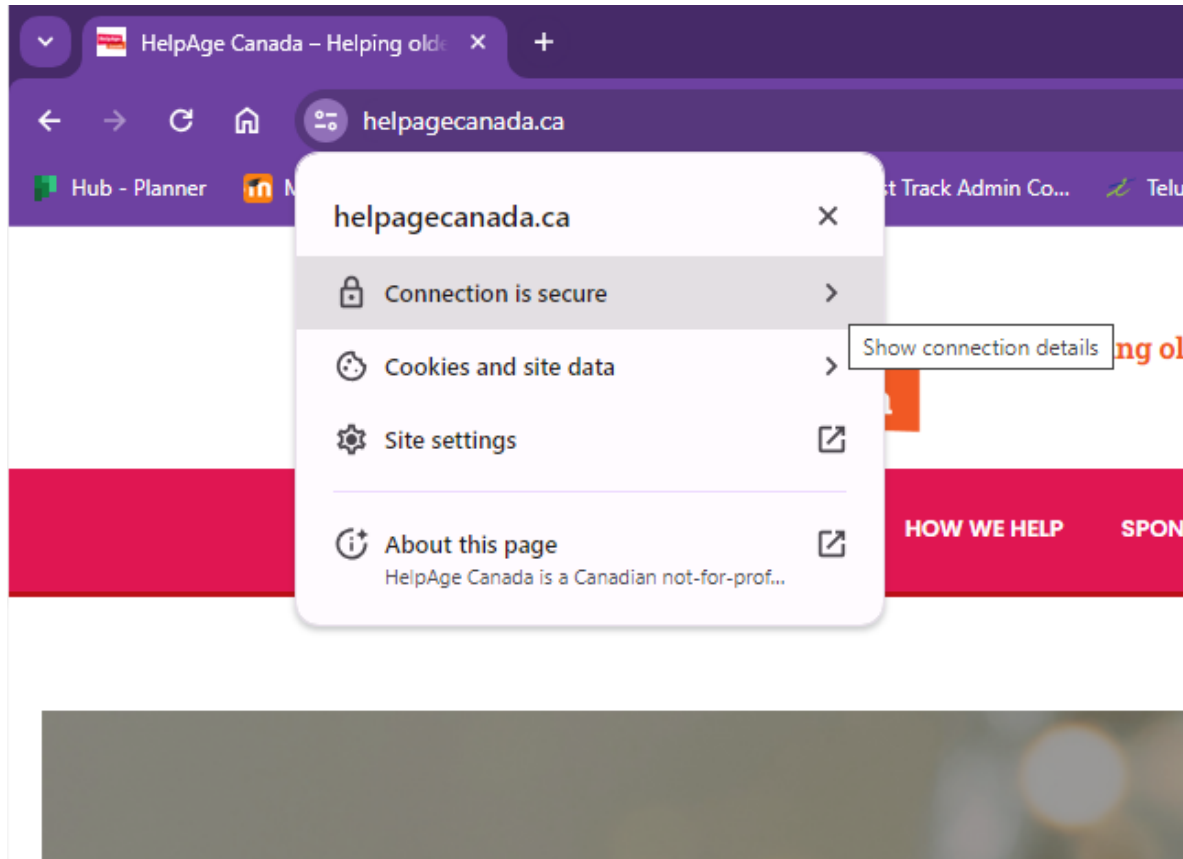
[Weight loss grants](#)

# Signs of a holiday scam

- You receive unsolicited emails or visit websites with grammatical errors, blurry logos or imperfect branding.
- You're pressured to spend money quickly, either to take advantage of a holiday sale/ offer or the caller asking for money in a hurry.
- You receive or purchase a gift card with the security code exposed on the back.
- You're asked to pay through methods that are difficult to reverse like wire transfers or prepaid cards (including gift cards).
- The site you're purchasing from isn't secure (the closed padlock symbol is missing from the web address) or is missing key information such as 'Contact Us'



# Secure Site



# Avoid a holiday scam

- Always check the URL
- Be cautious about hard-sell tactics or vague language
- Never pay for anything with a gift card
- Stick to reputable stores online as much as possible, or do research if wanting to purchase from a smaller retailer: a Google search of “[Company name] + scam” is a good start
- Any email/ text that you didn’t request should be treated with caution
- Contact a person or company directly
  - Never give personal information when you have been contacted directly
- Track deliveries through the company’s official website

***If it’s too good to be true, it probably is***



# AI Voice Scams

---

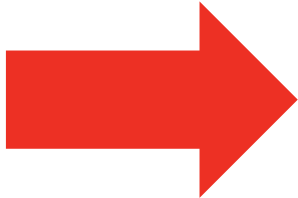
Voice related phone scams accounted for 30 per cent of the 106,000 fraud reports received by the Canadian Anti-Fraud Centre in 2021.

With the emergence of new tools, losses are going up significantly, from C\$165 million in 2020 to C\$531 million in 2022. In 2023, that figure is expected to tip over C\$600 million.

**Unfortunate Story**



# The Evolution of Scams



*“As the cost of deception slides towards zero, we will need to build our individual and societal immune systems to handle an army of new threats.*

*An ounce of prevention is worth a pound of cure.*

***The best vaccination for scams is knowledge and a sizable dose of skepticism.”***

# Part of the Problem: Isolation



One of the most common symptoms of social isolation **is not having anyone to discuss important things with.** [8]

As a result, **seniors who have been victimized by identity thieves are less likely to tell anyone about it,** making them attractive targets for criminals who want to avoid prosecution.



Whether living independently or in a community, loneliness is a common affliction for the elderly, making it even more likely for them to be preyed upon by identity thieves.

# What is the impact?

**Younger people reported losing money to fraud more often than older people.**

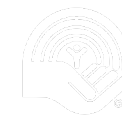
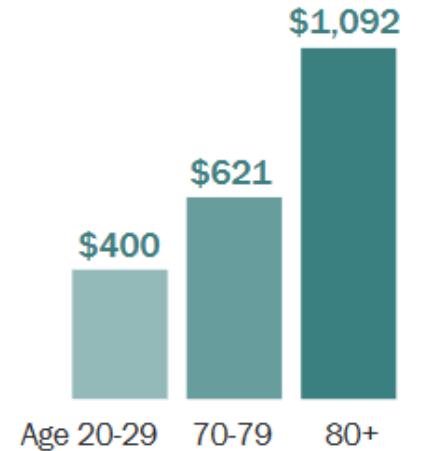


Age 20-29



Age 70+

**But when people aged 70+ had a loss, the median loss was much higher.**



United Way  
British Columbia

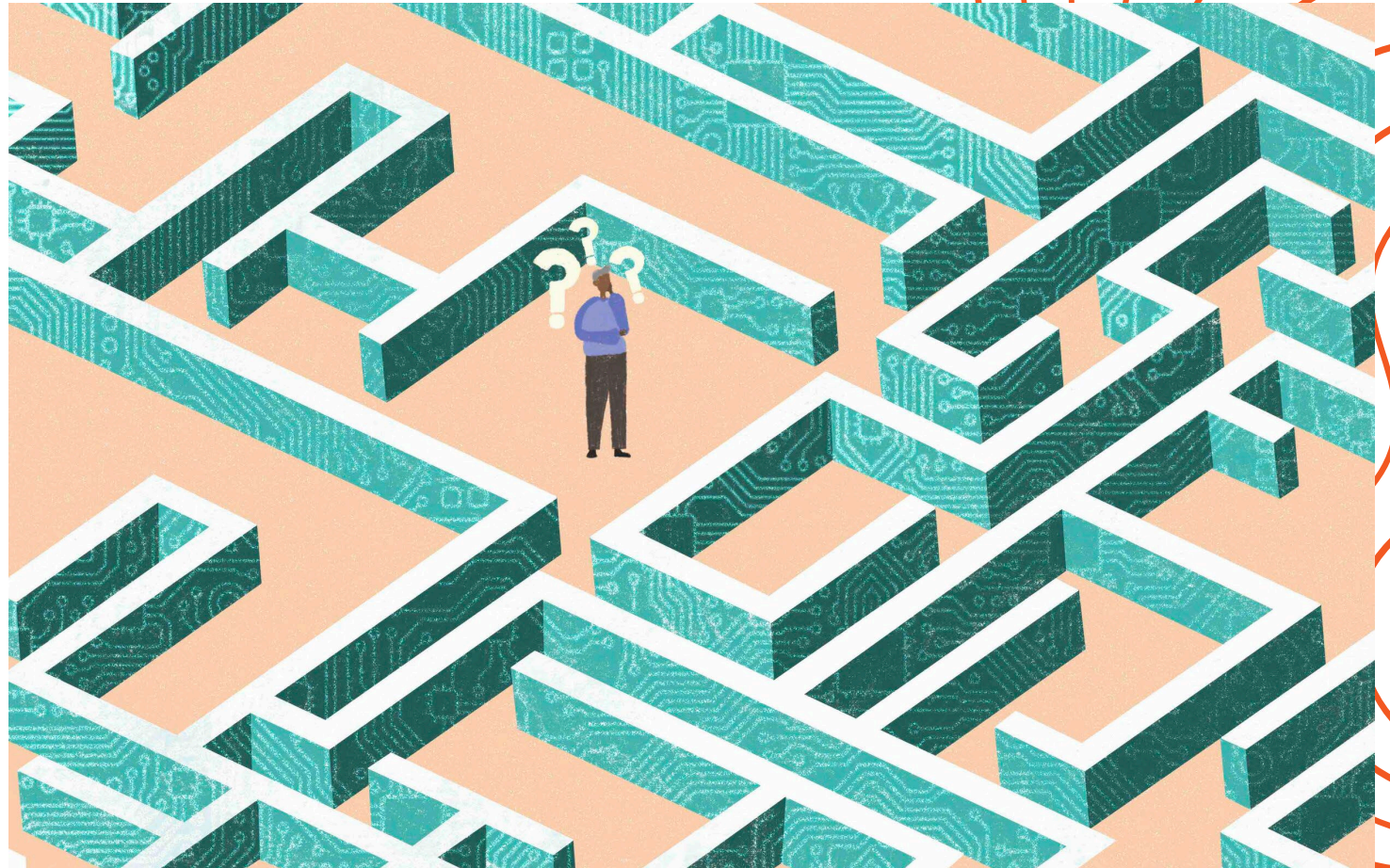
Working with communities in BC's  
Interior, Lower Mainland, Coastal,  
& Northern Vancouver Island



# What can we (CBSS Agencies) do to help?

---

- Support in building Digital Literacy.
- Share information about scams.
- Share tips to avoid scams.
- Empower families & support circles
- Share helpful tools and resources.
  - [Google Safe Site Status](#)
  - <https://www.youtube.com/user/cdnbankers/videos>



# Feature Resource



## How To Be Unscammable

A brand new series to help older adults stay one step ahead of cybercriminals

Two YouTube video thumbnails for the series 'How To Be Unscammable'. The first thumbnail is for Episode 3, titled 'All about the Dark Web', and the second is for Episode 4, titled 'Safely manage passwords'. Both thumbnails feature a woman with long brown hair and a red play button icon. Below each thumbnail is a blue button with white text: 'Episode 3 Show Notes →' and 'Episode 4 Show Notes →'.

Episode #3 • Has you...  
HOW TO BE UNSCAMMABLE  
All about the Dark Web

Episode #4 • Safely ...  
HOW TO BE UNSCAMMABLE  
Safely manage passwords

Episode 3 Show Notes →


Episode 4 Show Notes →

**Episode 3 • All About The Dark Web**

If your personal information has been stolen, the Dark Web is likely where it will be sold to cybercriminals. In this episode, I explain the Dark Web, show you how to see if your personal data is down there, and the next steps to

**Episode 4 • Safely Manage Passwords**

Your passwords are often the only thing between your data and cybercriminals. In this episode, I show you how to use secure passwords and share my Password Manager app recommendations. A must-watch

 **Gluu Society**

# What if you are a victim?

---

**1.** If you do share personal information, contact your financial institutions to place a fraud alert on your accounts.

Credit bureaus can also put a fraud alert on your account, which will alert lenders and creditors of potential fraud: [Equifax Canada](#); [TransUnion Canada](#)

**2.** Stay on alert and remember that you will likely be targeted again in another fraudulent way.

**3.** Report details to your financial institution(s), the [police](#) and/or [Canadian Anti-Fraud Centre \(CAFC\)](#).





# New Cyber Crime Reporting System

- RCMP & [Canadian Anti-Fraud Centre](#) (CAFC) are developing a new reporting system.
- Once fully in place, in 2023-2024, a victim or witness of a cybercrime or fraud will be able to use this system to report the crime online.

**HELP MAKE IT AGE FRIENDLY!**

<https://report.con.rcmp-grc.gc.ca/recruitment>

# CORE Canada & CORE BC





# CORE Tech Resource Library

## Common Naming Convention

### Library to include:

- Articles
- Educational Resources
- Podcasts
- Tutorials
- Apps
- Videos
- Etc.

The image displays a grid of six resource cards from the CORE Tech Resource Library. Each card is a rectangular tile with a header image, a title, a source, and a 'READ MORE' link.

- Card 1 (Top Left):** Header image shows hands holding a smartphone with floating envelope icons. Title: "[Article] What Spoofing Means and How to Stay Safe". Source: BC CRNS. Link: READ MORE →
- Card 2 (Top Middle):** Header image shows the Best Buy logo and the word "Digit". Title: "[Course] Best Buy Digital Citizen Online Courses". Source: Best Buy Canada. Link: READ MORE →
- Card 3 (Top Right):** Header image shows the ABC Internet Matters logo and the text "Searching safely online". Title: "[Resource] Internet Safety and Security: Searching Safely Online". Source: ABC Life Literacy Canada. Link: READ MORE →
- Card 4 (Bottom Left):** Header image shows the GETCYBERSAFE.CA logo and text: "Get Cyber Safe is a national public awareness created to inform Canadians about cyber sec the simple steps they can take to protect the online." Title: "[Resource] Get Cyber Safe". Source: Government of Canada. Link: READ MORE →
- Card 5 (Bottom Middle):** Header image shows a laptop screen with the text "Internet Safety & Security for Older Adults". Title: "[Resource] Internet Safety: Video Series". Source: South Okanagan Seniors Wellness Society. Link: READ MORE →
- Card 6 (Bottom Right):** Header image shows the Cyber-Seniors logo and the text "How to use NETFLIX". Title: "[Tutorial] How to Use Netflix For Seniors". Source: Cyber-Seniors. Link: READ MORE →

# Thank You

1. Thank you for joining us.
2. Stay tuned for more Webinars in the new year, based on your feedback!
3. CORE postings, please check regularly and use the discussion boards.



## For questions please contact:

Cheryl Baldwin – United Way of British Columbia

[CherylB@uwbc.ca](mailto:CherylB@uwbc.ca)

Nicole Perry – HelpAge Canada

[nperry@helpagecanada.ca](mailto:nperry@helpagecanada.ca)

## Contact Info

### You can always reach your Regional Community Developer:

#### ***Lower Mainland, Sea to Sky and Fraser Valley***

Dr. Beverley Pitman

[beverleyp@uwbc.ca](mailto:beverleyp@uwbc.ca)

604.969.8331

#### ***Vancouver Island/Gulf Islands***

Terry Harrison

[terryh@uwbc.ca](mailto:terryh@uwbc.ca)

250.514.1064

#### ***Interior BC***

Jessica Kleissen

[jessicak@uwbc.ca](mailto:jessicak@uwbc.ca)

604.969.8411

#### ***Northern BC***

Sarrahs Storey

[sarrahs@uwbc.ca](mailto:sarrahs@uwbc.ca)

250.699.1681

# Endnotes/ Resources

- “Tips for Staying Safe and Secure Online.” *AARP*, 7 May 2019, <https://www.aarp.org/home-family/personal-technology/info-2019/privacy-for-seniors.html>
- “Internet Safety for Seniors.” *Age Safe Canada*, 6 Apr. 2019, <http://agesafecanada.ca/internet-safety-for-seniors/>
- “Fraud Protection for Seniors.” *CPA Canada*, <https://www.cpacanada.ca/en/public-interest/financial-literacy/financial-literacy-education/request-a-session-in-your-community/seniors-sessions/fraud-protection-for-seniors>
- “Seniors Guidebook to Safety and Security.” *Royal Canadian Mounted Police*, 1 Nov. 2017, <https://www.rcmp-grc.gc.ca/en/seniors-guidebook-safety-and-security#a7-1>
- “Guides for Seniors from Connectsafely.” *ConnectSafely*, 26 Aug. 2021, <https://www.connectsafely.org/seniors/>
- Jeff Clune October 12, 2023. “Ai-Enabled Scams Will Proliferate.” *Macleans.Ca*, 26 Oct. 2023, [www.macleans.ca/society/technology/ai-scams/](http://www.macleans.ca/society/technology/ai-scams/)
- “How to Be Unscammable.” *Gluu Society*, [www.gluusociety.org/unscammable](http://www.gluusociety.org/unscammable)

# Endnotes/ Resources

- “Top Cybersecurity Threats for Seniors.” *AT&T Cybersecurity*, <https://cybersecurity.att.com/blogs/security-essentials/top-cybersecurity-threats-for-seniors>
- “Seniors Too Ashamed to Report Financial Fraud, Say Experts.” *CPA Canada*, 15 June 2018, <https://www.cpacanada.ca/en/news/canada/2018-06-15-seniors-too-ashamed-to-report-financial-fraud>
- “Online Safety.” *Alzheimer Society of Canada*, <https://alzheimer.ca/en/help-support/im-caring-person-living-dementia/ensuring-safety-security/online-safety>
- “Privacy Tips for Older Adults.” *Stay Safe Online*, 9 Apr. 2019, <https://staysafeonline.org/stay-safe-online/managing-your-privacy/privacy-tips-older-adults/>
- “Seniors 2021 Fraud Prevention Toolkit.” *Canadian Anti-Fraud Centre*, 15 Feb. 2021.
- “Top 10 Financial Scams Targeting Seniors.” *The National Council on Aging*, 19 Feb. 2021, <https://www.ncoa.org/article/top-10-financial-scams-targeting-seniors>
- Foran, Pat. “Ontario Man out \$8K in Scam That Uses AI to Mimic Voices of Friends and Family.” *Toronto*, CTV News, 23 Aug. 2023, [www.toronto.ctvnews.ca/ontario-man-out-8k-in-scam-that-uses-ai-to-mimic-voices-of-friends-and-family-1.6531933](http://www.toronto.ctvnews.ca/ontario-man-out-8k-in-scam-that-uses-ai-to-mimic-voices-of-friends-and-family-1.6531933)



# Endnotes/ Resources

- “Protect Yourself from Holiday Purchase Scams.” CIBC, [www.cibc.com/en/privacy-security/banking-fraud/frauds-and-scams/holiday-purchase-scams.html](https://www.cibc.com/en/privacy-security/banking-fraud/frauds-and-scams/holiday-purchase-scams.html)
- “Canadian Telecom Summit: Ai Taking Phone Fraud to New Heights: It World Canada News.” *IT World Canada - Information Technology News on Products, Services and Issues for CIOs, IT Managers and Network Admins*, 14 Nov. 2023, [www.itworldcanada.com/article/canadian-telecom-summit-ai-taking-phone-fraud-to-new-heights/552628#:~:text=Plus%2C%20they%20are%20relying%20heavily,use%20fully%20AI%2Dgenerated%20audio](https://www.itworldcanada.com/article/canadian-telecom-summit-ai-taking-phone-fraud-to-new-heights/552628#:~:text=Plus%2C%20they%20are%20relying%20heavily,use%20fully%20AI%2Dgenerated%20audio)
- Tietsort, J.R. “How to Avoid the 15 Most Common Holiday Scams (2023 Update).” *RSS, Aura*, 8 Nov. 2023, [www.aura.com/learn/holiday-scams#:~:text=Warning%20signs%20of%20holiday%20phishing,infect%20your%20device%20with%20malware](https://www.aura.com/learn/holiday-scams#:~:text=Warning%20signs%20of%20holiday%20phishing,infect%20your%20device%20with%20malware)