FRAUD PREVENTION TOOLKIT FOR SOUTH ASIAN SENIOR WOMEN

PROTECTING AGAINST FRAUDS AND SCAMS

IWIN IMMIGRANT WOMEN'S INFORMATION NETWORK

IWIN IMMIGRANT WOMEN'S INFORMATION NETWORK

IMMIGRANT WOMEN'S INFORMATION NETWORK (IWIN) HAS DEVELOPED A TOOLKIT TO ASSIST SOUTH ASIAN SENIOR WOMEN IN RECOGNIZING SCAMS AND TAKING PROACTIVE MEASURES TO SAFEGUARD THEIR PERSONAL INFORMATION AND FINANCES FROM FRAUD. THIS TOOLKIT CAN BE DOWNLOADED FROM THE IWIN WEBSITE FREE OF CHARGE. ADDITIONALLY, SELECTED SECTIONS ARE AVAILABLE IN URDU AND PUNJABI AS VIDEOS ON IWIN'S SOCIAL MEDIA PLATFORMS. PLEASE CIRCULATE WIDELY AMONG YOUR NETWORKS.

AT IWIN, WE ARE COMMITTED TO PROTECTING VULNERABLE COMMUNITIES FROM FINANCIAL SCAMS. BY WORKING WITH COMMUNITY ORGANIZATIONS, WE ENSURE THAT SOUTH ASIAN SENIOR WOMEN, ESPECIALLY IMMIGRANT WOMEN, HAVE THE TOOLS THEY NEED TO SAFEGUARD THEIR FINANCES, ASSETS, AND INVESTMENTS. OUR TOOLKIT PROVIDES SIMPLE STEPS AND PRACTICAL TIPS TO HELP THEM PROTECT THEMSELVES FROM FRAUD AND SCAMS.

Table of contents

IWIN IMMIGRANT WOMEN'S INFORMATION NETWORK

INTRODUCTION TO FRAUD PREVENTION

Fraud and scams can affect anyone, but older adults — particularly women from immigrant communities — face unique challenges.

As we navigate the complexities of modern life, it's essential to stay informed and aware of potential risks to our well-being. This toolkit is a guide to help South Asian senior women. It will show you how to protect yourself in the following ways:

1. Recognize potential scams.

- Be cautious about urgent requests for money or personal information.
- Be wary of unknown links or phone calls offering you prizes or making threats.

2. Protect your personal and financial information.

- Never share your social insurance (SIN) number or banking details over the phone or by email.
- Use strong passwords and shred sensitive documents before disposal.

3. Seek support and take action confidently if needed.

- Report scams to the Canadian Anti-Fraud Centre or local police.
- Notify your bank immediately if you suspect fraud.

UNDERSTANDING FRAUD AND ITS IMPACT

Fraud occurs when someone uses deceptive methods to take money, personal information, or other valuables. Scammers often target individuals they believe to be trusting or unfamiliar with certain technologies. For South Asian senior women, factors like language, cultural practices, or community connections may make scams harder to detect.

Why is this important?

From our community conversations, we learned that:

- many scammers exploit individuals' trust, respect for authority, or social obligations.
- Fraud can lead to emotional stress, financial challenges, and feelings of isolation.

IWIN IMMIGRANT WOMEN'S INFORMATION NETWORK

UNDERSTANDING FRAUD AND ITS IMPACT

REMEMBER, BEING CAUTIOUS DOES NOT MEAN BEING DISTRUSTFUL. IT MEANS PROTECTING YOURSELF AND THOSE YOU CARE ABOUT.

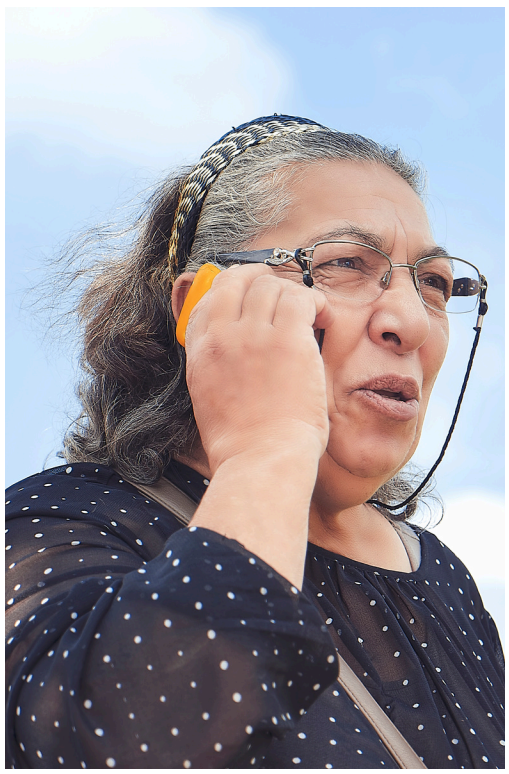
Regularly reviewing simple yet essential steps to safeguard your money and personal information is a proactive way to stay protected against fraud and scams.

While banks and the Government of Canada employ advanced technology and multiple layers of security to protect us, there are still important actions you can and should take to ensure your own safety.

We hope this resource serves as a trusted companion, empowering you to make informed decisions while fostering open conversations within your families and communities.

RESEARCH OVERVIEW

Practical Safety Measures



1. Secure your devices

Keep your phone, tablet, and computer safe by installing trusted antivirus and anti-malware software. Regularly update your devices to ensure you're protected against new threats. Set updates to install automatically so you never miss important security patches.

2. Be careful about what you share online

Scammers use personal information shared online to impersonate individuals or access accounts. To protect yourself, avoid publicly sharing sensitive details like your date of birth, address, or financial information, and only provide such information to trusted individuals or organizations you contact first.

3. Safely dispose of sensitive documents

Before throwing away old financial or personal documents, take steps to ensure they can't be used by scammers. Shred or tear up items like bank statements, credit card bills, or other papers with personal details to prevent them from falling into the wrong hands.

4. Use strong and unique passwords

Create unique, hard-to-guess passwords for each online account and avoid reusing them to enhance security. If you suspect a password is compromised, change it immediately for that account and any others using the same password.

Fraud and scams are not just financial crimes — they have emotional, psychological, and social consequences.

On the basis of insights from focus group discussions and recent research, we have identified common scam tactics that target older adults, particularly immigrant women:

- **Phishing/email scams**
- **Immigration deportation scam**
- **Community or cultural scams**
- **Phone or voicemail scams**
- **Lottery/prize scams**
- **Tech support scams**
- **Family emergency or grandparent scams**

IWIN IMMIGRANT WOMEN'S INFORMATION NETWORK

TOOLKIT CHECKLIST

Common types of scams

Phishing/email scams

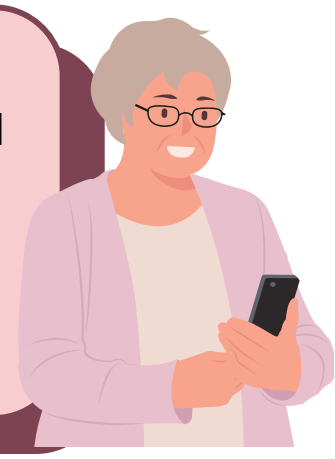
What happens: Scammers send fake emails or text messages pretending to be from a trusted source like a bank, government agency, or utility company.

Example:
An email claims to be from your bank, warning that your account will be locked unless you verify your password.

How to stay safe:
Avoid clicking on links in unexpected messages.
Contact the organization directly to confirm.

Phone or voicemail scams

What happens: Scammers pretend to be from the government or a utility company and say you owe money or your information is at risk.



Example:
Someone calls saying they are from the Canada Revenue Agency (CRA) and demands payment or threatens legal action.

How to stay safe:
Hang up and call the real organization.
Don't share personal details like your SIN or bank info.
Ignore threatening voicemails.

Immigrant deportation scam

What happens: Scammers target individuals with threats related to immigration status, demanding money to avoid deportation or legal action.

Example:
"This is the immigration department. Your status is under review, and you must pay $2,000 immediately to prevent deportation."

How to stay safe:
Remember that government agencies will never demand payment over the phone.
Contact the official immigration department directly to confirm any claims.

Prize and lottery scams

What happens: Someone says you've won a prize but need to pay fees to claim it.

Example:
"You've won a car! Send $500 to cover the taxes."

How to stay safe:
Legitimate prizes do not require payment.
Be wary of offers that seem too good to be true.

IMMIGRANT WOMEN'S INFORMATION NETWORK

TOOLKIT CHECKLIST

Common types of scams

continued

Family emergency or grandparent scam

What happens: Someone pretends to be a family member in trouble, asking for urgent financial help.

Example: "Nani, I've been in an accident, and I need money for the hospital. You can't tell anyone else, or I will be in trouble ."

How to stay safe:
Verify the caller's identity by asking personal questions that only your family member would be able to answer.
Reach out to other family members to check the story.

Community or cultural scams

What happens: Scammers exploit trust during religious or cultural events to ask for donations.

Example:
A fake charity asks for contributions during Diwali or Ramadan.

How to stay safe:
Research charities before donating.
Only give to known and verified organizations.

Tech support scams

What happens: You get a call or pop-up saying your computer is at risk, asking you to pay for "help."

Example:
A pop-up displays, "Warning: Your computer is infected! Call this number now."

How to stay safe:
Avoid calling numbers from unsolicited pop-ups.
Use trusted local repair services for technical issues.

PRACTICAL TIPS FOR PROTECTION

Steps to recognize and avoid scams

Red flags to look for	How to protect yourself
Pressure to act quickly: Scammers may insist on immediate payment or decisions.	**Pause and verify:** Take a moment to think. Contact someone you trust to review the situation.
Requests for confidential information: Scammer may ask for passwords, PINs, or bank details.	**Avoid sharing personal information:** Keep your banking details and identification private.
Secrecy: Scammers may discourage you from discussing the matter with others.	**Check credibility:** Always verify the identity of callers or organizations before responding.

Practical tips for protection

1. Personal information

- Use strong passwords or passphrases for online accounts.
- Safely dispose of documents containing personal details by shredding them.
- Limit how much private information you share on social media.

2. Financial awareness

- Check your bank statements regularly for unusual activity.
- Never send money through wire transfers or prepaid cards to individuals you don’t know.
- Be cautious of fundraisers or charities unless you have verified that they are legitimate.

3. Technology safety

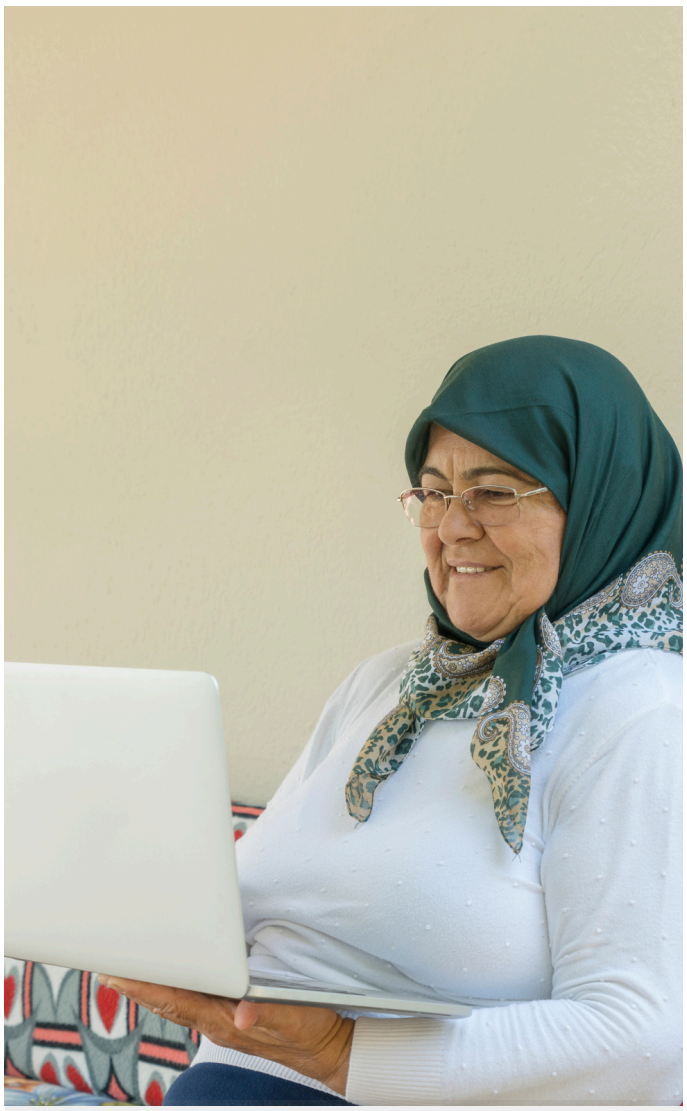
- Keep your computer and phone updated.
- Install antivirus software.
- Avoid downloading unknown apps or clicking on suspicious links.

Checklist: simple steps for staying safe

- [ ] Verify the identity of anyone requesting personal or financial information.
- [ ] Regularly check bank statements for unauthorized transactions to detect scams early.
- [ ] Avoid clicking on links or attachments in unexpected emails or texts.
- [ ] Report suspicious activity immediately.
- [ ] Share concerns with a trusted friend or family member.
- [ ] Let unknown calls go to voicemail to avoid scam pressure and verify the caller.

PROTECTING YOURSELF AGAINST FRAUD

Protecting yourself against fraud starts with awareness and simple actions. This page provides practical tips and resources to help you stay safe, supported, and empowered in your community.



Fraud prevention is a shared responsibility. Learn how to safeguard your personal information, lean on your community for support, and take action if you suspect a scam.

Support from your community and family

Strengthening family connections

- Talk openly with family members about scams and fraud.
- Ask for their help if you're uncertain or confused about something.

Building community awareness

- Attend fraud prevention workshops at local centres or places of worship. Share what you learn with others in your community.

What to do if you're targeted

- **End contact:** Politely stop communication with the individual or organization.
- **Collect information:** Save emails, texts, or other evidence.
- **Report the scam:**
  - Canadian Anti-Fraud Centre: 1-888-495-8501
  - Seniors Safety Line: 1-866-299-1011
  - Gather evidence: Save all communications as proof.

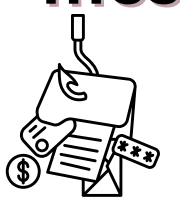
Remember, reporting fraud helps to protect others in your community and stop fraudsters.

IWIN IMMIGRANT WOMEN'S INFORMATION NETWORK

Your Scam Detection Guide: A Step-by-Step Tool to Stay Safe

Use this guide to evaluate any suspicious calls, messages, or requests. Follow these steps to identify red flags, verify information, and take the right actions to protect yourself from scams.

Follow these steps to evaluate suspicious calls, emails, or messages.



Evaluate the request

- Be wary of requests for personal details (passwords, SIN, banking info).
- Avoid sending money via gift cards or wire transfers.
- If requests seem emotional, verify with someone else first.
- Take a moment to assess if the situation feels urgent or unexpected, as scammers exploit pressure.
  - ie. Your bank will never ask for your PIN over the phone.

Identify red flags

- Scammers pressure quick action and warn of consequences for delays.
- Be cautious with unknown senders or callers using threats or excessive friendliness.
- Refuse to keep the situation secret—it's a major red flag.
- Offers that seem "too good to be true," like lottery winnings, are likely scams.

Pause and verify

- Take your time; scammers want you to rush.
- Contact the organization directly using official numbers or websites.
- Consult a family member, friend, or community leader for advice.
- Research the request online (e.g., search "CRA scam") to check for known fraud.

Please evaluate us!

Let us know what you think.
Your input is very important to us. Please complete this brief survey on your thoughts on this tookit:

Scam Toolkit Survey

ACKNOWLEDGEMENTS

We thank all the participants of our focus groups for their time and for their invaluable contributions to this research. This toolkit would not have been possible without their feedback. We also thank Ansa Talat (program coordinator) and Human Endeavour for setting up the focus groups.

FUNDING

The development and publication of this toolkit was made possible through funding from the Government of Canada's New Horizons for Seniors Program (NHSP). The views expressed herein do not necessarily represent the views of the funder.

IWIN IMMIGRANT WOMEN'S INFORMATION NETWORK

CONTACT US!

info@iwinca.ca

www.iwinca.ca

Contact us to join our membership!

Funded by:

Canada

New Horizons for Seniors Program

DISLAIMER

IWIN has strived to provide information that was accurate and up to date at the time of publication. However, this resource should not be considered financial and legal advice. All decisions regarding finances are up to the discretion of the individual. Any opinions expressed herein may not reflect the policies or views of IWIN or any partners or funders.