# Be a Savvy Senior

## Fraud Protection Strategies for Seniors on **Identity Theft**

fact sheet 5

**Con artists use your strengths against you. They target seniors because you are trusting, optimistic, and courteous about responding to correspondence.**

**Be savvy about fraud: Spot it. Stop it.**

### Phishing and Malicious Software

*Bernadette is checking her email. She sees that she has a message from UPS with the subject heading: "Tracking number 76290X00P4Q38Z". She opens the email. It explains that her order has arrived: she just has to click on the link below, and enter her personal information to finalize the delivery of her package. Bernadette doesn't recall ordering anything recently, but her birthday is coming up... maybe the package is from her cousin in Arizona?*

**SPOT IT!**

- You get an email from what appears to be your bank, a utility or a familiar business
- Clicking on the email will send you to a fake website, which may look very real—or that website may look "off" or have spelling mistakes
- If you enter your account information, credit card details, or password, the con artists capture that private information with a computer program
- Sometimes the fake website will contain a virus that will infect your computer and provide another person with access to your personal files

**STOP IT!**

- Do not reply to the email or phone any number the email lists
- Use only phone numbers, email addresses and customer service numbers found in old bills from that agency. Look up numbers in the phone book or online. Contact them to investigate directly.
- Don't click on any web-links contained in an email unless you know the sender
- Review the policies of organizations you have online business with. Banks have clear policies about not sending emails to customers.
- Run regular virus scans and quarantine suspicious files. You can download virus scan programs for free, or you can purchase this type of software.

**Computers: You can learn—don't get burned!**

**Scammers randomly target email addresses hoping for a response. Sharing personal information online increases your risk of identity fraud.**

# Be a Savvy Senior

Fraud Protection Strategies for Seniors on **Identity Theft**

## Telemarketing and Text Message Scams

*Joan gets a text message on her phone telling her that she has won a prize: an all expenses paid trip to San Francisco! To claim the prize she is asked to click on a link. The link takes her to a website where she is asked to provide personal information such as her full name, her birth date and her Social Insurance Number (SIN). She fills in the information and writes back "Who is this?" Before she knows it her identity has been stolen—someone is out there impersonating her. They use her information to get credit cards, make purchases, change billing information and even take out an application to remortgage her home!*

### SPOT IT!

- You get a text or phone call from an unknown number offering you a prize
- Claiming the "prize" requires you share personal information, bank accounts, passwords or identity numbers
- Sometimes the text message or phone call will be from a person claiming to work for your financial institution (bank, credit union), or a utility (hydro, cable) or government agency. They may say they are calling you because your account has been compromised.

### STOP IT!

- Keep your Social Insurance Number, birth certificate, passport, and all other key personal information in a safe place.
- Do not reply to these messages, even to say, "No, thank you", "Who is this?" or "Don't contact me again". Once you reply they have your information.
- If you are worried about the security of an account, find an old bill and call that financial institution, utility or agency directly
- Never use any link provided in an unknown text or email
- Lock your mailbox to prevent mail theft
- Empty your mailbox regularly
- Shred documents that may contain personal information—thieves troll in your trash!

**Mum's the word—guard your personal information.**

Don't share PINs, passwords, your SIN number or other personal identifiers. Only provide addresses and phone numbers to people you trust.

**To report frauds and scams, call:**

1. Your local police force or RCMP attachment, or
2. The Canadian Anti-Fraud Centre at 1.888.495.8501

CANADIAN CENTRE FOR ELDER LAW

Centre for Public Legal Education Alberta

Government of Canada / Gouvernement du Canada

Canada