Internet Scams Targeting Older Adults

Canadian seniors are increasingly being targeted by sophisticated internet scams.

Index

Why are seniors being targeted?

Seniors are particularly vulnerable because they tend to be trusting, have less computer skills, and are less likely to report fraud.

As a result. financial scams often go unreported and they can be tough to prosecute as they're viewed as "low-risk" crimes.

Examples of internet scams

1) The Grandparent scam

Scammers often target grandparents by calling and pretending to be their grandchild. They might say something like, "Hi, Grandma, do you know who this

is?" When the unsuspecting grandparent guesses the name of the grandchild the scammer most sounds like, the scammer is able to instantly secure their trust. The fake grandchild then asks for money to solve some urgent financial problem.

2) Impersonation scams

Scammers may pose as government or bank staff, family members, law enforcement, or other trusted people.

3) Sweepstakes and lottery scams

Scammers call an older adult to tell them they've won a lottery or a prize. To claim their winnings, they must send money or gift cards up front to cover taxes and processing fees.

4) Computer Tech support scams

Technical support scams prey on older people's lack of knowledge about computers and the internet. A pop-up message or warning screen appears on a computer or smartphone, telling the user their device is damaged and needs fixing. When they call the support number for help, the scammer may request remote access to the older person's computer and demand they pay a fee to have it repaired.

5) Romance scams

Romance scammers create fake profiles, often on social media, and exploit older adults' loneliness to get money.

6) Phishing scams

Beware of phishing emails and text messages that may seem to come from a familiar bank, credit card company, or online store. These messages often ask for an older adult's personal data, such as login credentials or Social Security number, under the pretense of verifying their account or updating their credit card information. However, scammers use this information to steal money or additional personal information.

7) Investment scams

This scam involves the illegal or alleged sale of financial instruments that typically offer low risk and guaranteed returns.

8) Gift Card Scams

Be wary of online sellers or billers who demand payment in the form of a gift card. They may request you to buy a gift card and share the card number and PIN. Remember, gift cards are meant for gifting and not for making payments. Any individual requesting a gift card as payment is likely to be a scammer.

9) Invoice Scams

Individuals who receive an unexpected invoice should always contact the sender directly by finding their email or phone number online. They should not use the contact information provided on the invoice, as it is likely to be fake.

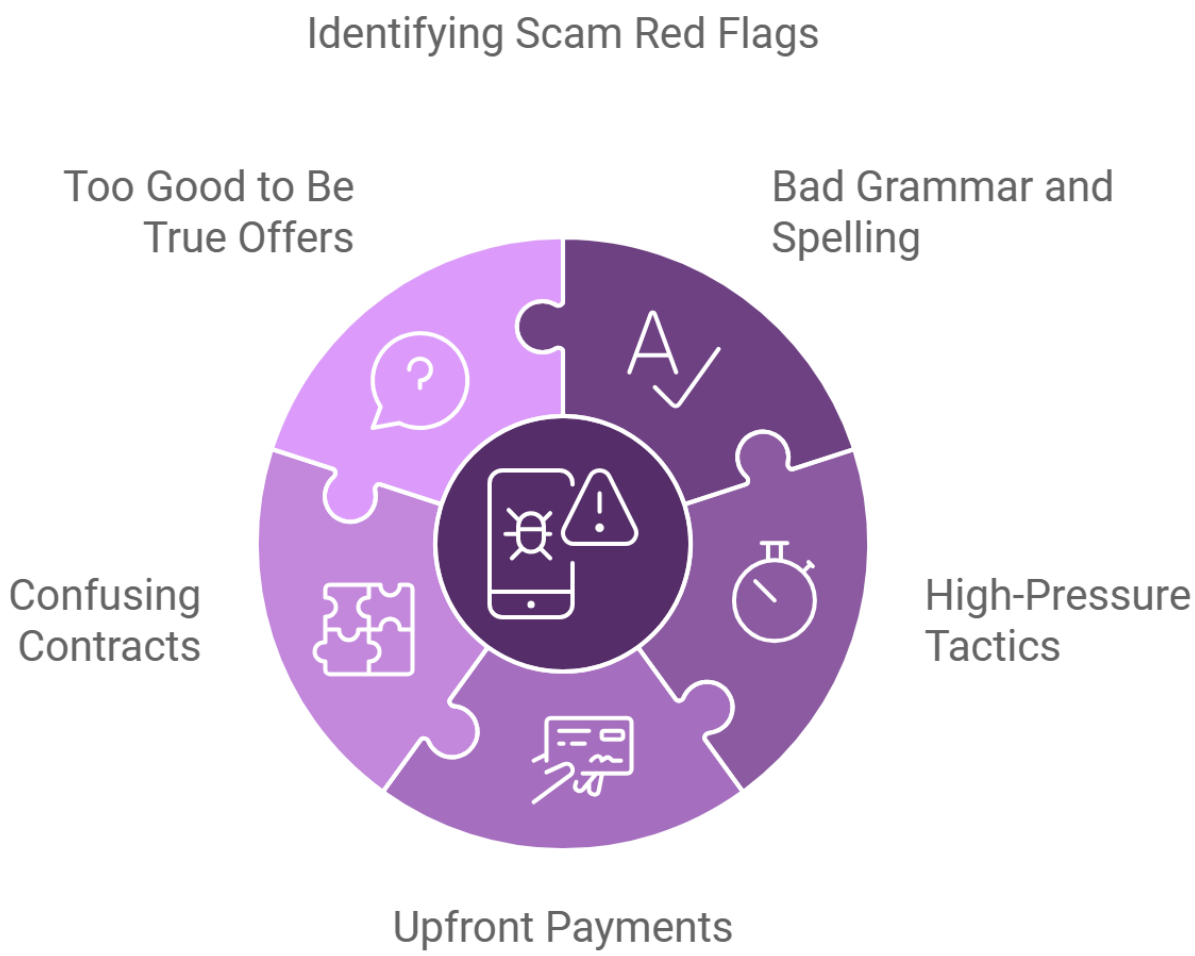
10) Credit Repair Scams

Beware of credit repair scams that claim to improve your credit by removing negative information from your report for a fee. It's important to know that legitimate negative information cannot be removed from your credit report, regardless of how much you pay.

How to Spot a Scam

There are a few red flags that you should be aware of: bad grammar and spelling, high-pressure tactics, upfront payments, confusing or non-existent contracts, and the offer - that is just “too good to be true.”

Fortunately, there are many simple steps you can take to help you stay safe online.



Simple steps to keep yourself safe

1) Never give out money or sensitive information by text or email. Be especially wary of Crypto Investments.

2) Never click on a link or download an attachment from an unknown source. Even if it looks legitimate, verify the sender before taking any action.

3) Keep your information secure using strong passwords and passphrases; and ensure your anti-virus software and internet browser are always up to date.

4) When online, don't enter login information or credit card details unless you are sure the site is legitimate. Red flags are a URL that doesn't match the company's

main site or a lack of a security lock symbol in the address bar.

5) Be especially wary if the requestor is pressing you to act quickly.

6) Stay connected to your finances and set up alerts for suspicious activity on your bank account or credit card

Last Updated: December 4, 2024

NICE - National Initiative for Care of the Elderly
www.nicenet.ca