## **Senior Frauds and Scams**

Infographic

#### **Common Scams**

#### **Phishing Scams**

Phishing is an attack where a scammer calls you, texts or emails you, or uses social media to trick you into clicking a malicious link, downloading malware, or sharing sensitive information.





# Tips on How to Protect Yourself

- Call the sender to verify legitimacy (e.g. if you receive a call from your bank, hang up and call them).
- Always be wary of links or attachments that you weren't expecting.
- Avoid sending sensitive information over email or texts.

#### **Grandparent Scam**

Grandparent scams (also called emergency scams) are common scams that target seniors. These scams usually involve a phone call from someone who pretends to be your grandchild.





- Never offer information to the caller.
- Ask the caller a few personal questions, press your caller for details.
- Never provide your credit card number over the telephone or Internet.
- Never wire money to someone under uncertain conditions.

### Phone or Voicemail Scams

You receive a call or a voicemail from a criminal who is posing as a government agency or member of law enforcement.





- If you receive a call from a scammer, hang up or delete the voicemail message.
- Block the caller's phone number and report the calls to the Canadian Anti-Fraud Centre.

#### **Romance Scams**

If you meet someone online but have not seen them in-person, and they begin to ask you for money, it's likely a romance scam.





- If your love interest asks you to send money, be very suspicious.
- Ask them for a recent photo or do a video call.
- Fraudsters often claim they are in another part of the world as the reason for not being able to meet in-person.

#### For more information

Elder Abuse Prevention Ontario 416-916-6728 | www.eapon.ca admin@eapon.ca | @EAPreventionON

# RESOURCES Canadian Anti-Fraud Centre www.antifraudcentre-centreantifraude.ca

Government of Canada www.cyber.gc.ca



