Protect Yourself from AI Scams & Deepfakes

A Safety Guide for Seniors

1. Common Scams Targeting Seniors

📞 Phone Scams

- **"Grandparent" scam:** Someone pretends your grandchild is in trouble and urgently needs money.
- **Fake government calls:** Claims you owe taxes, fees, or may be arrested.
- **Tech support scams:** Someone tells you your computer has a virus and needs "fixing."

💻 Online & Email Scams

- **Phishing emails** pretending to be from your bank, Canada Post, Amazon, etc.
- **Fake prize notices** requiring you to "pay a fee" to claim winnings.
- **Romance scams** using online dating or social media to gain trust and ask for money.

🏦 Financial & Investment Scams

- Pressure to invest in "guaranteed" high returns.
- Requests for **money transfers, gift cards, or cryptocurrency**.
- Fake charities asking for urgent donations.

2. What Are Deepfakes?

Deepfakes are fake videos, phone calls, or audio recordings created using artificial intelligence. They can make it look or sound like a real person, even a family member, when it is not.

Scammers can:

- Create a deepfake voice from **only 3–5 seconds** of audio.
- Make realistic videos of people asking for money or promoting fake investments.
- Use AI to impersonate bank staff, government agents, or loved ones.

3. Why Seniors Are Targeted

1.866.243.4301
Suite 150, 926 5th Avenue SW
Calgary AB T2P 0N7
bridgewaterbank.ca

Scammers often focus on older adults because:

- Seniors may have more savings.
- Many grew up trusting phone calls, photographs, and video.
- Emotional scams involving family are extremely effective.

4. Common Deepfake Scams Affecting Seniors

1️⃣ Grandparent Emergency Voice Scam

A caller sounds exactly like your grandchild and says:

"I'm in trouble — please send money now!"

2️⃣ Fake Videos of Public Figures

Deepfake videos of celebrities or politicians promoting fake investments or products.

3️⃣ Romance or Friendship Scams

AI-generated photos, videos, or voices used to build emotional trust.

4️⃣ Tech Support or Bank Impersonation Calls

AI-generated voices claim your account is compromised or your computer has a virus.

5. Warning Signs of Any Scam

🚩 General Red Flags

- Asked to keep something **secret**.
- Pressured to act **urgently**.
- Requests for **gift cards, e-transfers, crypto, or wire transfers**.
- Unusual pop-ups demanding payment.
- Spelling mistakes, suspicious links, or unknown email senders.

🚩 Deepfake Audio Warning Signs

- Voice sounds flat, robotic, or "too smooth."
- Strange pauses or unnatural rhythm.
- Highly emotional or urgent pleas.

🚩 Deepfake Video Warning Signs

1.866.243.4301
Suite 150, 926 5th Avenue SW
Calgary AB T2P 0N7
bridgewaterbank.ca

- Eyes blinking strangely or not blinking.
- Lips not matching the words.
- Lighting that looks inconsistent.
- Fuzzy edges or pixelation around the face.

6. How to Protect Yourself

✔ **Always Verify First**

- Hang up and call back using a **trusted phone number**.
- Verify with another family member if someone claims to be in trouble.
- Contact your bank or government directly — **never through numbers provided in suspicious messages**.

✔ **Guard Your Personal Information**

- Never share your **SIN, banking info, PIN, or passwords**.
- Do not click links or download attachments from unknown senders.

✔ **Slow Down**

Scammers want you to panic.
Real organizations **do not pressure you** to act immediately.

✔ **Use Strong Device Security**

- Keep devices updated.
- Turn on antivirus protection.
- Use strong, unique passwords.
- Enable **two-factor authentication (MFA)**.

✔ **Limit Personal Information Online**

- Reduce what is shared publicly (photos, dates, family names).
- Review Facebook, Instagram, and other privacy settings.

✔ **Be Cautious with Investments**

- If a celebrity or politician is promoting an investment, assume it's fake until verified.
- Check with your **provincial securities regulator** before investing.

1.866.243.4301
Suite 150, 926 5th Avenue SW
Calgary AB T2P 0N7
bridgewaterbank.ca

7. What To Do If You Suspect Fraud

🚫 Stop Immediately

- Stop all communication.
- Do NOT send money — no matter what they threaten.

📞 Report the Scam

- **Your bank or credit union**
- **Canadian Anti-Fraud Centre:** 1-888-495-8501
- **Local Police** (non-emergency line)
- **Online reporting:** https://reportcyberandfraud.canada.ca/

Even if you didn't lose money, reporting protects others.

8. Quick Safety Tips

- If it sounds too good to be true — it is.
- Government agencies **never** request payment in gift cards or cryptocurrency.
- Banks will **never** ask for your password or PIN.
- Let unknown numbers go to voicemail.
- Discuss unusual financial requests with a trusted friend or family member.

9. Helpful Contacts

📞 **Canadian Anti-Fraud Centre:** 1-888-495-8501
🌐 **Website:** www.antifraudcentre-centreantifraude.ca
👮 **Local Police:** Visit your local police website for non-emergency numbers
🏦 **Your Bank:** Use the phone number printed on your bank card

10. Remember: You Are Not Alone

If something feels wrong, **trust your instincts**.
It's okay to **hang up**, say **no**, or ask someone you trust for help.

1.866.243.4301
Suite 150, 926 5th Avenue SW
Calgary AB T2P 0N7
bridgewaterbank.ca