



There are many scammers and financial fraudsters in the world—many of whom target our vulnerable populations.

Vulnerable populations are part of our communities. They include our elders/seniors, youth, and those living with physical, mental or financial challenges. Here are some of the most common types of scams and financial frauds and tips on how to protect ourselves and our vulnerable community members.

COMMON SCAMS AND FINANCIAL FRAUD



MAIL/EMAIL SCAMS

- » Unsolicited email/mail advising that you are either the beneficiary of funds or winner of a lottery, gift cards or some type of sweepstakes.
- » This scam will ask you to pay upfront fees before money can be released.



PHISHING

- » The solicitation of personal or financial information from you by impersonating reputable organizations such as the CRA or a financial institutions.



COMPUTER TECH SUPPORT SCAMS

- » Fraudsters claim to be from a tech company such as Apple or Microsoft saying that your computer has been hacked and they need remote access to fix it, which can expose your personal information.
- » They will also ask for credit card information to charge a fee for the repairs.



ROMANCE SCAMS

- » Romantic attention via phone, mail, in-person, or by digital means with the aim of gaining access to and exploiting personal and financial information.



ABUSE OF TRUST

- » Family, friends and caregivers can also take advantage of you. In many cases, your personal and financial information is exploited for monetary gain.

TIPS TO HELP PROTECT FROM SCAMS AND FINANCIAL FRAUD



STAY VIGILANT

- » Fraudsters come in many different ways, so you have to be aware of mail, email, text messages, phone calls or people that make suspicious requests that sound too good to be true.



DON'T EXPOSE YOUR PERSONAL AND FINANCIAL INFORMATION

- » Be mindful about where you access confidential information and who you share it with. If you are unsure or suspicious about anything, please reach out to your local police service, First Nation office or other trusted organizations or persons.



BE SKEPTICAL OF HIGH-PRESSURE TACTICS OR THREATS

- » Fraudsters often employ high-pressure tactics or threats to coerce individuals into making hasty decisions. This may look like them asking you to make a payment or provide information within a deadline or 'limited time' opportunity. Take your time to research and evaluate any financial opportunities or investments before you decide what to do.



NEVER CLICK ON ANY LINKS RECEIVED FROM SUSPICIOUS SENDERS

- » Clicking on links from suspicious senders can expose you to various cyber threats, including malware, phishing, identity theft, financial scams, and compromised security.



ASK FOR HELP AND USE COMMUNITY RESOURCES

- » Seek assistance from trusted advocates, support groups, local shelters, outreach programs, and support services that can offer assistance in verifying suspicious requests and help protect yourself from scams and financial fraud.

