MOST COMMON SCAMS & FRAUD | SASCU

Here are the most common scams in the ever-changing fraud environment.

Phishing Scams

- Emails or texts that appear to be from legitimate companies asking for personal information or prompting the recipient to click on a malicious link.

Phone and Tech Support Scams

- **Impersonation:** Scammers pretend to be government officials, tech support, or even family members in distress to extract money or personal information. Common ones are 'Amazon', 'Best Buy', 'CRA'.
- **Robocalls**: Automated calls that promise prizes or threaten legal action to scare the recipient into providing information or payment.
- **Calls or pop-up messages** claiming the device has a virus and offering to fix it for a fee, often gaining remote access to the computer, or directing payment offline by gift cards, or cash by courier.

Marketplace Scams

- Fake items posted where the seller asks for deposit or full payment before meeting to see the item.
- E-transfer Buyer sends the seller a spoofed Interac payment that actually allows them to steal login credentials to send out unauthorized transfers, or request money fulfillment to fraudster's account.

Investment Scams

- Ponzi schemes or fraudulent crypto investment opportunities that promise high returns with little risk.
- Recovery scams offering to recover crypto losses by initial scam for a fee or remote account access.

Lottery/Sweepstakes and Charity Scams

- Notifications claiming the recipient has won a prize but must pay a fee or provide personal information to claim it. Number one red flag is it's for a contest you've never entered.
- Fake charities that solicit donations, especially after natural disasters or during the holiday season.

Health Care and Home Repair Scams

- Prescription drug scams: Offers for cheaper medications that are counterfeit or never delivered.
- Unsolicited offers for home repairs at a low price, often requiring upfront payment and then disappearing without completing the work. Common ones are duct cleaning, or driveway sealing.

Grandparent Scams

- Calls or texts from someone pretending to be a grandchild or relative in urgent need of money due to an emergency. Use of AI with sampled voice from social media make these especially hard to detect.

Romance Scams

- Online relationships where the scammer builds trust and then asks for money, often for fabricated emergencies.

TIPS TO PROTECT YOURSELF

SASCU

Stay Calm and Don't Panic: Scammers often try to create a sense of urgency. Take a moment to breathe and think before reacting. Tell them you'll need more time. Hang up, and verify the source, or call some-one you trust to let them know about the request.

Trust Your Instincts and Be Skeptical: If something feels off or too good to be true, it probably is. Trust your gut and verify before taking any action.

Do Not Engage and Hang Up or Delete: If you receive a suspicious call or message or pop-up, hang up or delete it without responding. Engaging can give scammers more information.

Verify the Source and Contact the Organization Directly: Use a verified phone number or website to con-tact the business or government agency to confirm the legitimacy of the communication.

Protect Personal Information: Do not provide personal or financial information over the phone, email, or text unless you are certain of the recipient's identity.

Report it:

- **Financial Institutions**: If financial information was shared, contact SASCU or the credit card company immediately. If unauthorized transactions occurred, they may be able to attempt recovery.
- **Local Authorities:** Report the scam to local law enforcement.
- **Canadian Anti-Fraud Centre:** Report by phone 1-888-495-8501 or online at CAFC website.

Monitor Accounts and use good tech "hygiene"

- Check Statements: Review bank and credit card statements for any unauthorized transactions.
- Set Up Alerts: Use account alerts to be notified of any unusual activity.
- Update Software: Ensure that your computer and smartphone have the latest security updates and an-tivirus software.
- Enable Two-Factor Authentication: Add an extra layer of security to your online accounts.

Seek Support and Talk to Someone: Tell a family member or friend. They can provide support and help you take the necessary steps.

Educate Yourself and Stay Informed: Keep up-to-date with common scams and tactics used by fraud-sters. Refer to local RCMP websites, Canadian Anti-Fraud Center and Better Business Bureau.

Has someone asked you to buy and send gift card codes to them?
Has someone asked you to withdraw cash and send it to them by courier?
Has someone asked you to withdraw cash and deposit it to a bitcoin ATM?
Has someone asked you to tell service reps a story such as it's for renovations?
STOP! These are all scam tactics to steal your money.

RESOURCES

SASCU

Canadian Network for the Prevention of Elder Abuse
https://cnpea.ca/en/

Canadian Anti-Fraud Centre
http://www.antifraudcentre-centreantifraude.ca/index-eng.htm

Federal/Provincial/Territorial Ministers Responsible for Seniors Forum
https://www.canada.ca/en/employment-social-development/corporate/seniors/forum.html

Speak Up! Advance Care Planning Campaign
http://www.advancecareplanning.ca