Quick Reference Guide, Page 1

Warning Signs		Prevention Tips
Urgent calls from "grandchildren" in trouble, requests for money transfers or gift cards	*GRANDPARENT SCAM*	Verify the caller's identity with personal questions. Contact other family members to confirm the story. Never send money based solely on a phone call.
Rapid emotional investment, reluctance to meet in person, requests for money	*ONLINE ROMANCE SCAM*	Be cautious of online-only relationships. Never send money to someone you haven't met in person. Use reverse image search to verify profile pictures.
Unsolicited offers, pressure for immediate decision, unusually low prices	*HOME REPAIR SCAM*	Get multiple quotes from licensed contractors. Verify contractor credentials and references. Never pay full amount upfront.
Notifications of winnings from contests you didn't enter, requests for fees to claim prizes	*LOTTERY SCAM*	Remember: legitimate lotteries never require upfront fees. Verify lottery claims through official channels. Be skeptical of unexpected "winnings".
Unsolicited offers for medical equipment, requests for Medicare information	*HEALTHCARE SCAM*	Verify offers with your doctor or local pharmacy. Never give out Health card ID/numbers to unsolicited callers. Be wary of "free" medical offers.
Unsolicited calls about computer problems, requests for remote access	*TECH SUPPORT SCAM*	Legitimate tech companies won't make unsolicited calls. Never give remote access to unknown individuals. Be wary of pop-up warnings with phone numbers.

Quick Reference Guide, Page 2

Warning Signs		Prevention Tips
High-pressure tactics, vague details about how donations are used	*CHARITY SCAM*	Verify charities through official sources before donating. Be cautious of charities with names similar to well-known organizations. Don't be pressured into immediate donations.
Promises of high returns with low risk, pressure to invest quickly	*INVESTMENT SCAM*	Be skeptical of "guaranteed" high-return investments. Check the credentials of any investment professional. Take time to research before investing.
Threatening calls from "tax agencies", demands for immediate payment	*INCOME TAX SCAM*	Know that tax agencies never demand immediate payment over the phone. Verify tax information through official channels. Be wary of unsolicited calls about taxes.
Unsolicited requests for personal information, unexpected account changes	*IDENTITY THEFT SCAM*	Never give out personal information to unsolicited contacts. Regularly monitor your credit report and bank statements. Use strong, unique passwords for all accounts.
Promises to eliminate debt quickly, requests for upfront fees	*DEBT RELIEF SCAM*	Be wary of guarantees to fix credit problems. Check with a credit counselor for legitimate debt relief options. Avoid companies that require large upfront fees.
Pressure to buy unnecessary services, inflated prices	*FUNERAL SCAM*	Know your rights regarding funeral services. Get itemized price lists from multiple funeral homes. Don't be pressured into making immediate decisions.

Term Index

A
Anti-virus Software: Programs designed to detect, prevent, and remove malicious software from computers and devices
Authentication: The process of verifying the identity of a user or system

B
Breach: Unauthorized access to data or systems
Bulk Email Fraud: Mass distribution of fraudulent emails hoping to deceive recipients

C
CAFC: Canadian Anti-Fraud Centre, Canada's central agency for reporting fraud
Catfishing: Creating a fictional online persona to deceive others
Cryptocurrency: Digital or virtual currency often used in investment scams
Cybersecurity: Practices protecting systems, networks, and programs from digital attacks

D
Dark Web: Hidden websites that require special software to access
Data Mining: Collecting personal information for fraudulent purposes
Digital Footprint: Trail of data you create while using the Internet

E
Encryption: Process of coding information to prevent unauthorized access
E-transfer Fraud: Scams involving fraudulent electronic money transfers

F
Fraud Alert: Warning placed on credit files to prevent identity theft
Phishing: Attempting to obtain sensitive information by posing as a trustworthy entity

G
Gift Card Scam: Fraud involving the purchase and transfer of gift card codes
Grooming: Process of building trust with potential victims over time
Guaranteed Investment: Often used as bait in investment scams

Term Index

H
Hacking: Unauthorized access to computer systems or data

I
Identity Theft: Criminal use of another person's personal information
Investment Fraud: Deceptive practices related to financial investments

J
Junk Mail: Unsolicited emails often containing scams or malicious links
Joint Account Fraud: Unauthorized access to shared bank accounts

L
Lottery Scam: False claims of lottery winnings requiring upfront fees
Liability: Legal responsibility for financial losses due to fraud

M
Malware: Malicious software designed to damage or gain unauthorized access
Money Mule: Person who transfers illegally acquired money on behalf of others
Multi-Factor Authentication: Enhanced security requiring multiple verification methods

N
Network Security: Protection of computer networks from cyber threats
Next of Kin Scam: Fraud claiming inheritance from unknown relatives
Non-Disclosure Agreement (NDA): Often misused by scammers to silence victims

O
One-Time Password (OTP): Automatically generated code used for authentication
Online Banking Fraud: Unauthorized access to online banking accounts

P
Password Manager: Software that stores and manages online credentials
Personal Information: Sensitive data that could be used to identify an individual

Term Index

R
Romance Scam: Fraudulent scheme exploiting romantic intentions
Red Flag: Warning sign indicating potential fraudulent activity

S
SIN: Social Insurance Number, a confidential Canadian identification number
Smishing: Phishing attempts via SMS text messages
Spoofing: Disguising communication to appear from a trusted source
Security Questions: Backup verification method often targeted by scammers

T
Two-Factor Authentication (2FA): Security process requiring two forms of identification
Tech Support Scam: Fraudulent scheme claiming to offer technical assistance

U
URL Manipulation: Altering web addresses to deceive users
Unauthorized Transaction: Financial activity not approved by account holder

V
Virus: Malicious code that can copy itself and corrupt computer systems

W
Wire Transfer: Electronic transfer of money often requested by scammers
Whaling: Phishing attacks targeting high-profile individuals