Protect yourself from losing money to cybercrime

Managing Your Money

LYNN MacNEIL

Cybercrime has become one of the most common and costly threats facing Canadians today. The scale of the problem is difficult to overstate, and new research continues to show how pervasive and damaging digital fraud has become across the country.

According to new data from the non-profit Angus Reid Institute, the situation is more widespread than many people realize. Their findings show that more than four-in-five Canadians say they have faced a phishing or fraud attempt in the past two years—often by phone, email, text message, or online (www.angusreid.org, January 2026). About 30 percent reported having money or personal information stolen, and those aged 60+ are almost twice as likely as adults under 30 to have been victimized. Across income levels there is almost no difference. Canadians of all financial backgrounds are being targeted. According to Angus Reid, it's hard to get accurate statistics on these crimes because only five to 10 percent of cases are reported.

These statistics paint a sobering picture: being targeted is now the norm, and a significant portion of the population, especially older adults, are losing real money.

As a wealth advisor, I've spent my career helping people build and protect their financial security. I've helped clients navigate market downturns, sudden life events, and unexpected emergencies. But one threat stands out as uniquely devastating: modern financial scams.

Just recently, a long-time client shared a heartbreaking story. Her friend, a woman in her eighties, widowed, cautious, and financially responsible, lost her entire life savings to what's known as the "gold bar scam." Believing she was protecting her assets, she withdrew her investment accounts and handed the money over to criminals posing as legitimate authorities. She told no one what she was doing, convinced that secrecy was necessary and that she was following official instructions. By the time her family realized what had happened, the money was gone. Wealth that was built over decades was erased in days.

When I looked into the mechanics of the scam, I was struck by how professionally orchestrated it was. These are not simple phishing emails or amateur attempts. Many of these criminals are part of organized networks trained in persuasion, psychology, AI-generated voices, and impersonation. They study how Canadians speak, how major institutions communicate, and how to generate panic without raising suspicion.

Anyone can be fooled, and victims often feel ashamed or embarrassed, which only keeps the problem hidden. But knowledge is protection. Knowing how these scams operate can help you protect yourself from being caught up in the scheme.

Below are the most effective, easy-to-follow strategies across all major channels: phone, email, text, social media, messaging apps, and even in-person attempts.

PHONE SCAMS

Phone scams remain one of the most dangerous forms of fraud because trained callers can sound authoritative and convincing.

Common Red Flags:

- Caller claims to be from CRA, your bank, police, Amazon, Microsoft, or a courier service
- Claims there is a crime linked to your personal information
- Urgent commands: "Do not hang up," "Stay on the line," "Keep this confidential"
- Requests for gift cards, crypto, cash withdrawals, or "verification payments"

What to Do:

- Hang up immediately. Legitimate institutions do not demand urgent action by phone.
- Never call back the number they give you—look up the official number yourself.
- **Tell someone**. Scammers isolate victims by pushing secrecy.

A Script to Use:

"I do not handle financial or security matters over the phone. I will contact the institution directly myself."

Then hang up. A legitimate representative will support this decision and be understanding.

TEXT AND EMAIL SCAMS

Digital messaging scams are becoming increasingly sophisticated, often impersonating well-known brands or government agencies.

Red Flags:

- Slight misspellings in email addresses
- Attachments or links you weren't expecting
- "Verification" requests
- Messages impersonating Canada Post, Costco/Best Buy, banks, Netflix/Amazon, or government programs

What to Do:

- Never click links in unsolicited texts or emails and delete suspicious messages.
- If a text includes a link, assume it's a scam. Legitimate institutions do not send clickable links to fix urgent problems.
- Use multi-factor authentication (MFA) on all financial accounts.
- If a message appears to be from a friend, call them to confirm they actually sent it.

If it appears to be from an institution and might be real, look up the phone number yourself—never trust contact information in the message.

SOCIAL MEDIA SCAMS

Criminals have increasingly turned to social platforms to target Canadians.

Common Tactics:

- Fake investment or crypto opportunities
- Romance scams
- Fraudulent marketplace listings
- Impersonation of friends, family, or influencers

How to Protect Yourself:

- Never send deposits or payments to someone you haven't met in person.
- Communicate through official platform messaging—avoid moving to private apps.

Research the account: new profiles with few connections are a major red flag.

Be suspicious of high-return, no-risk "investment opportunities."

BANKING & INVESTMENT SAFEGUARDS

These steps can significantly reduce your risk of financial loss:

- Enable Account Alerts - Set up daily withdrawal and transfer notifications so you are instantly aware of unusual activity.
- Use Account Restrictions – Some banks allow "view-only" modes or daily transfer limits to reduce exposure.
- Strengthen Verification - Ensure your investment firm cannot withdraw funds based solely on an email request. The best practice is a personal phone call from someone who knows your voice.
- Appoint a Trusted Contact - Most investment firms now offer a "trusted contact person" option—especially valuable for seniors.

The most important piece of advice is *slow down*. Scammers rely entirely on urgency. Take a pause before acting on any request for money or personal information.

Cybercrime is no longer a niche threat affecting the careless or the unlucky. It is widespread, sophisticated, and increasing every year. The Angus Reid Institute's findings make it clear: Canadians of all ages and income levels are being targeted—and many are losing money.

But with awareness, skepticism, and a few strong personal security habits, you can dramatically reduce your risk. Talk openly with family members, especially older adults, about common scams. Share this information widely – with friends, neighbors, and your community.

Protecting your financial future isn't only about saving and investing wisely.

It's also about understanding and recognizing the threats that can take everything in an instant.

For a printable checklist with these tips and more, visit our Useful Tools page at https://mvewealth.com/useful-tools

Note: For more tips and insights on managing your wealth, follow me on my Facebook page **MVE Wealth**.

Lynn MacNeil, F.PL., CIM®, is a Senior Wealth Advisor and Portfolio Manager with Richardson Wealth Limited in Montreal, with over 30 years of experience working with professionals and pre-retirees. For a second opinion, private financial consultation, or more information on this topic or on any other investment or financial matter, please contact Lynn MacNeil at 514.981.5796 or Lynn.MacNeil@RichardsonWealth.com. Or visit our website at www.MVEWealth.com