



# CANADIAN ANTI-FRAUD CENTRE BULLETIN

20 Years of Fraud – Solicitation Methods

2024-03-11

FRAUD: RECOGNIZE, REJECT, REPORT

This year marks the 20<sup>th</sup> anniversary of Fraud Prevention Month. The theme of this year’s campaign is **“20 years of fighting fraud: From then to now.”** With this theme, we’ll be exploring how certain frauds have evolved with the rise of the digital age, drawing insightful comparisons between the past and present.

This bulletin was prepared to highlight some of the main solicitation methods based on reporting received at the Canadian Anti-Fraud Centre (CAFC). Most of the solicitation methods used by fraudsters today existed 20 years ago, but how they are using them has evolved.

Below are the top solicitation methods based on the initial contact used by fraudsters:

## **Telephone**

Based on the number of reports received in 2023, the telephone was the top solicitation method used by fraudsters. Over the last 20 years, technology related to fraudulent telephone calls has evolved. Fraudsters are now able to spoof phone numbers, automate calls and make “robo” calls. The evolution in technology has given fraudsters the ability to target many more Canadians over the last number of years. Fraudsters will commonly claim to be loved ones, law enforcement, financial institutions, or government agencies.

## **Cyber-Enabled Fraud (Email, Internet, Social Media and Text Message)**

With more than 75 % of reported losses associated to cyber-enabled fraud in 2023, the CAFC emphasizes how the cyber environment has changed over the last 20 years and how this has affected fraud.

Fraudsters have added social media platforms as one of their main tools to target victims. Whether they’re using fraudulent ads, compromised social media accounts, and social media bots to collect personal information, fraudsters have taken advantage of social media to target Canadians.

Though electronic mail fraud existed 20 years ago, fraudsters today have taken advantage of technology at their disposal allowing them to make fraudulent emails more convincing. Email address spoofing in phishing and infiltrating networks before a spear phishing attack have added complexity to email fraud.



Royal Canadian Mounted Police  
Gendarmerie royale du Canada



Competition Bureau  
Canada

Bureau de la concurrence  
Canada



Ontario Provincial Police

Canada

## **Mail**

While regular post mail fraud has decreased substantially over the last 20 years, the CAFC continues to receive reports of fraud initiated by mail. Fraudulent mail can come in the form of a fake inheritance letter claiming that you are entitled to a large sum of money because a distant relative has died. Fraudsters also send fraudulent prize letters claiming you've won the "big prize." Once you call the phone number in the letter, fraudsters will ask for payments to cover fees or insurance.

## **Door to Door / In Person**

Fraud initiated in person is very similar to what it looked like 20 years ago. Fraudsters might offer a service with little to no value or ask you to sign a contract for equipment that doesn't work properly. Fraudulent contractors might offer home improvement services such as roofing, driveway paving, or landscaping at a low price. Door-to-door fraudsters commonly use high-pressure sales tactics. Once payment, deposit, or prepayment is received, they disappear or provide a service of poor quality.

## **Warning signs and how to protect yourself**

- Criminals use call-spoofing to mislead victims. Don't assume that phone numbers appearing on your call display are accurate.
- If you receive a suspicious or odd message from a trusted friend, contact them through a different means of communication to confirm that it's actually them.
- If you get an unsolicited email or text asking you to click a link or open an attachment – don't do it!
- If contacted by a company, don't use the contact information provided in the message. Look up the legitimate contact information elsewhere and contact it directly.
- Use reputable service providers located in your area.
- Locate and verify the service provider's contact information –address, phone number, email—before paying for the service.
- Be wary of letters offering you an inheritance. These letters will often claim to come from lawyers or accountants.
- If you receive or letter claiming you've won a free prize, know that you are not required to pay up front fees to collect winnings.
- Learn [more tips and tricks for protecting yourself.](#)

If you suspect you've been the victim of cybercrime or fraud report it to your local police and to the CAFC's [online reporting system](#) or by phone at 1-888-495-8501. If not a victim, report it to the CAFC anyway.