CANADIAN ANTI-FRAUD CENTRE BULLETIN

Uncovering fraud:
Lifting the lid off the fraudster's toolbox 2025-03-10

FRAUD: RECOGNIZE, REJECT, REPORT

March is Fraud Prevention Month #FPM2025, and the Canadian Anti-Fraud Centre (CAFC) will focus on **uncovering fraud**—revealing the tactics criminals use to create convincing identities, impact on victims and what we are doing to fight fraud. Fraudsters are experts at disguising themselves and creating false identities to manipulate, deceive, and steal from their victims. By exposing these deceptive practices, we aim to empower Canadians to spot fraud before it happens.

Fraudsters are becoming increasingly sophisticated, using advanced tools and tactics to deceive their victims. This week, we're diving into the tools of the trade that fraudsters rely on, with a focus on social engineering, emerging technologies, and fraudulent documents. Understanding their methods is the first step in protecting yourself, family and loved ones.

We have compiled a list and explanation of some of the most common tools we found in the fraudster's toolbox:

Social engineering

Fraudsters are masters of exploiting human psychology. They rely on emotional manipulation, creating scenarios that push victims to act without thinking which puts them in a vulnerable situation. Common tactics include:

- **Phishing:** Sending fake emails or messages that appear to be from trusted organizations to steal personal or financial information.
- **Impersonation fraud:** Pretending to be someone you trust, such as a government official, tech support, or a family member in distress.
- **Urgency and fear:** Creating a false sense of urgency to pressure victims into making quick decisions, such as paying a fake bill or providing confidential information.

Technological tools

As technology continues to evolve, so do the fraudsters' tactics. They leverage tools such as:

- **Dark web resources:** Fraudsters use the dark web to buy and sell stolen data, fake identities, and malware tools.
- **Artificial intelligence (AI):** AI tools can generate realistic voices, deepfake videos, and convincingly fake text, making fraud harder to detect.
- **Spoofing software or websites:** Technology that allows fraudsters to mimic legitimate phone numbers, emails, or websites.

Fake identification (ID) and documents

Fraudsters often use fake IDs, passports, and other documents to carry out their frauds. These tools can be used to:

- commit ID fraud

    - open fraudulent accounts
    - account takeovers
    - apply for loans
    - apply for credit cards and cellphones
    - government benefit fraud
- bypass verification processes
- make them appear credible in all types of fraud

Warning signs – How to protect yourself

- Be wary of unexpected requests for personal or financial information. Take a moment to verify the source
- Learn to recognize the signs of phishing, impersonation, and all types of fraud. Don`t forget to share what you learn with family members and loved ones
- Use strong, unique passwords and enable two-factor authentication wherever possible
- Regularly check your financial and online accounts for unauthorized activity
- If your personal information has been compromised (identity theft), follow the steps listed on the CAFC website to protect yourself from being a victim of identity fraud

Anyone who suspects they have been the target of cybercrime or fraud should report it to their local police and to the CAFC's online or by phone at 1-888-495-8501.