Fraudulent Ads on Social Media Increasingly Targeting National and Local Online Users

Executive Summary

CyberAlberta Threat Intelligence is aware of a recent surge in fraudulent ads appearing on various social media platforms targeting Canadians at a national and local level. These campaigns -- operated by financially motivated threat actors -- leverage impersonation tactics, social engineering, and generative AI to deceive victims into divulging sensitive financial and personal information.

Two campaigns specifically targeted Albertans, with one impersonating the Alberta.ca website to offer fake Canada Carbon Rebate (CCR) payments via fraudulent ads on Facebook, while another spoofed Red Deer's MyRide transit system to harvest personal and financial data. Nationally, Canada's news outlets and major banks are being impersonated by fraudulent ads leveraging generative AI to produce audio deepfakes and fake user endorsements for fake or fraudulent investment platforms. Recommendations to help organizations respond to these and similar campaigns are provided at the end of this report.

Introduction

Online Fraud campaigns leveraging social media ads are on the rise across Canada, with targets ranging from national audiences being lured by impersonations of banks and even the Prime Minister, to residents of local municipalities in Alberta being enticed with fraudulent public services. A recent CyberAlberta report highlighted that the Government of Alberta (GoA) has been impersonated in malicious ads spread on Facebook offering CCR payments. Initially considered a singular event, subsequent incidents suggest this is part of a growing trend involving multiple unknown threat actors engaged in online scams. This latest report provides insights into the four known fraud campaigns targeting Canadians, outlining the tactics, techniques, and procedures (TTPs) employed by these actors, including the use of AI-generated content to rapidly produce convincing lures that enhance their social engineering efforts.

Albertan-Specific Targeting

Impersonation of the Government of Alberta to Offer Fake Canadian Carbon Rebates

Beginning as early as June 3rd, Alberta residents were targeted by fraudulent ads on Facebook impersonating the GoA, claiming to offer CCR payments. These ads directed users to site content hosted on the malicious domain **albertagov[.]ca**. This campaign aimed to harvest sensitive personal information, including Social Insurance Numbers, Alberta.ca credentials, and security questions such as mothers' maiden names, likely with the intent to faciliate subsequent fraudulent activity.

Figure 1 - CCR scam impersonating the GoA on Facebook

In total, CyberAlberta Threat Intelligence attributed this campaign to one IP address listed below and the four associated domains, all of which were registered through NameSilo.

IP Address: **47.239.216[.]183** owned by Alibaba US Technology (AS45102)

Associated Domains:

- **albertagov[.]ca**
- **ccr-alberta[.]com**
- **ccr-alberta[.]info**
- **myalbertaccr[.]ca**

Resolving the domain **albertagov[.]ca** in a browser shows a fake login portal that directs users to ‘Sign in to check eligibility’ in order to harvest Alberta.ca credentials.

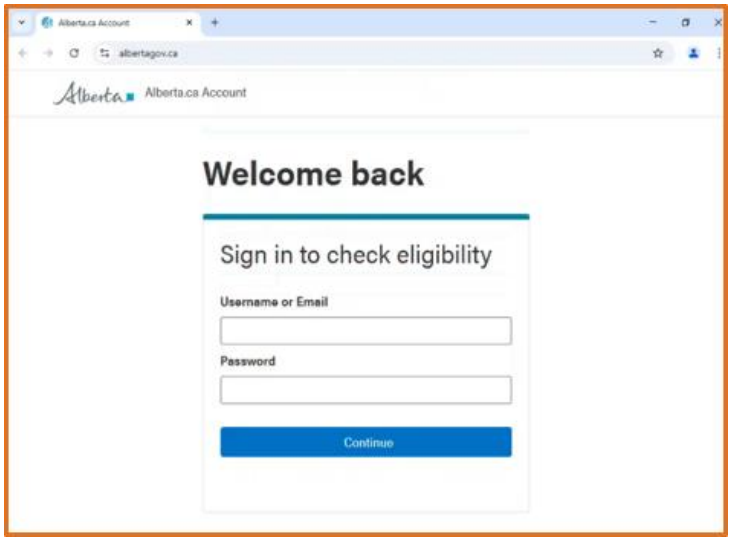

Figure 2 - Screenshot of albertagov[.]ca when resolved in a browser. Site content shows a sign in portal impersonating the Government of Alberta, attempting to steal alberta.ca credentials under the pretense of checking eligibility for CCR payments.

Hunting For Similar Infrastructure

Proactive searches identified additional domains with active certificates registered through NameSilo that appear to impersonate legitimate Alberta-based entities. Several of these domains host AI-generated content designed to either initiate contact with users or defraud them by leveraging the legitimate Stripe payment platform for illegitimate services. While these assets are not currently linked to a single coordinated campaign, they underscore the persistent threat posed by online scams targeting local populations. Moreover, they highlight how generative AI facilitates the rapid development and deployment of fraudulent websites and content.

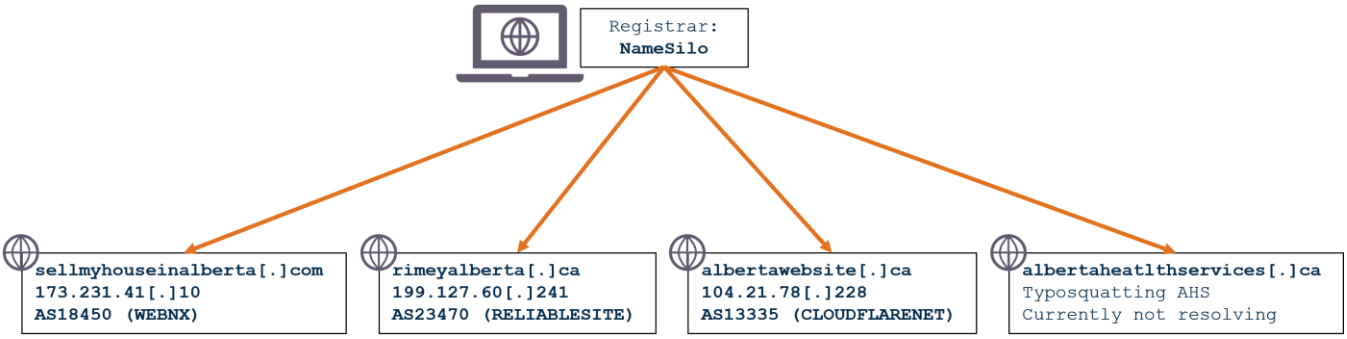

Figure 3 - Scam websites with active certificates registered through NameSilo impersonating alberta-based entities.

Residents of Red Deer Targeted by Fake Transport Scheme

The City of Red Deer's cybersecurity team recently identified a fraudulent advertising campaign active since June 16th, targeting local residents on Facebook. This campaign impersonates the city's legitimate MyRide transit fare system, enticing users with an offer of a six-month free transit pass. To create a sense of urgency, the ads present the promotion as a limited time offer with a finite number of available passes. The scam is disseminated through a Facebook account titled “Public Transport in Red Deer,” which uses the city's official logo and other images from their site to enhance credibility. The intent of this campaign is to harvest personal and financial information by directing users to complete a form, following a series of questions and a pre-designed challenge that always results in success, potentially resulting in further financial fraud at the victim’s expense.

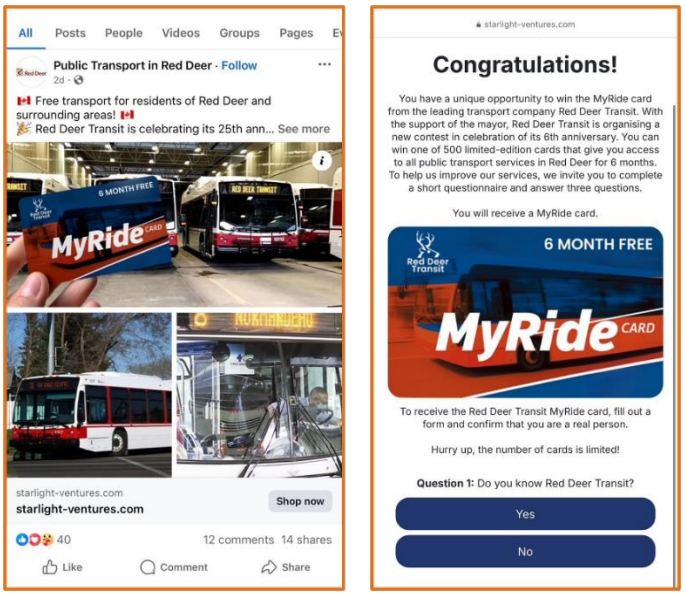

Figure 4 - Fraudulent ad impersonating the city of Red Deer's MyRide transit far system.

The fraudulent campaign is hosted on the domain **`startlight-ventures[.]com`**, registered via Squarespace. As of this writing, the domain resolves to **`92.53.111[.]163`**, an IP address allocated by Selectel (AS 49505), a

Russian based virtual proxy provider known for hosting malicious infrastructure and exhibiting resistance to takedown actions.

This incident underscores the increasing sophistication of financially motivated threat actors, who are investing substantial effort into reconnaissance and the creation of highly convincing lures. While this campaign targeted residents of Red Deer, it is highly likely that similar tactics are being deployed against other municipalities across Alberta and Canada. These developments emphasize the urgent need for elevated public awareness, both nationally and within regional and municipal communities.

Nationwide Targeting

Fake Articles Luring Canadian Users into Investment Scams

CyberAlberta Threat Intelligence recently identified a surge in fraudulent ads on the social media platform X, promoting an investment scam aiming to commit financial theft. These ads, posted by “verified” user accounts, impersonate Canadian news outlets such as CBC News, posting fake articles with sensationalist headlines designed to capture user interest.

The ads use shortened Bitly links that redirect to pages hosted on the **`mindfultech[.]live`** domain. These fake articles purport to be a recounting of a press conference where Prime Minister Mark Carney allegedly endorses an investment scheme called “Immediate Spike,” urging Canadians to invest $355 with promises of guaranteed returns. In reality, “Immediate Spike” is a fraudulent platform, no such endorsement or press conference occurred, and CBC News has never published this content.

Figure 5 - Flow Diagram illustrating how online users are directed to the investment scam Immediate Spike.

To enhance perceived legitimacy and simulate authentic engagement, threat actors generated fabricated testimonials attributed to fake personas, including references to reputable Canadian organizations. These were accompanied by comments from fake users with Canadian-themed usernames, all praising the scam platform and providing additional links to it. Generative AI was likely used to produce both the profile images and the text content shown in Figure X, illustrating how AI enables threat actors to rapidly create convincing impersonations, contextually enriched to target specific demographics.

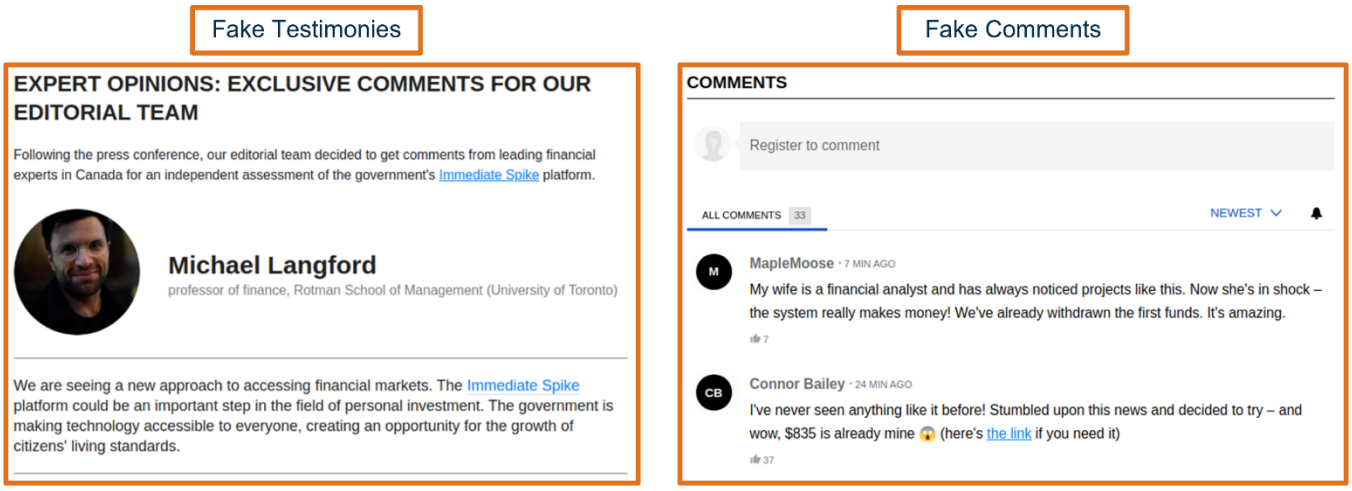

Figure 6 - AI-enabled fake testimonials and user comments on the impersonating CBC News article hosted on mindfultech[.]live

Canadian Banks Impersonated in Instagram Ads Attempting Financial Fraud

On June 17th, BleepingComputer reported a wave of fraudulent ads on Instagram impersonating major Canadian banks to facilitate financial fraud. These ads served multiple purposes, some sought to steal online banking credentials, while others enticed users to join a "private WhatsApp investment group." Although the specific follow-on tactics within the WhatsApp group remain unclear, it is likely that harvested contact details are used for targeted social engineering to enable further fraudulent activity.

One campaign impersonating EQ Bank offered personal and business accounts with abnormally high interest rates to entice users. Victims who clicked the ad were redirected to **`auth.rbcpromos1[.]cfd`**, a credential-harvesting site specifically tailored to EQ Bank users. However, the presence of "rbc" in the malicious domain suggests the presence of similar campaigns impersonating the Royal Bank of Canada (RBC).

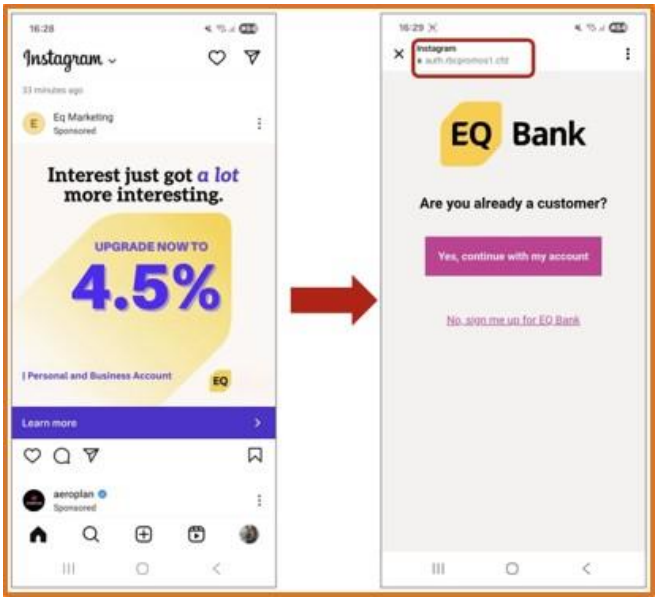

Figure 7 - Fraudulent ad on Instagram impersonating EQ Bank.

Another observed campaign misappropriated the identity of Brian Belski, the Bank of Montreal's (BMO) Chief Investment Strategist. This ad, deployed via Instagram Stories under the name "BMO Belski," used the built-in Polls feature to pose investment-related questions in an apparent effort to simulate engagement and build trust. Users who interacted with the poll were then prompted to submit their contact information.

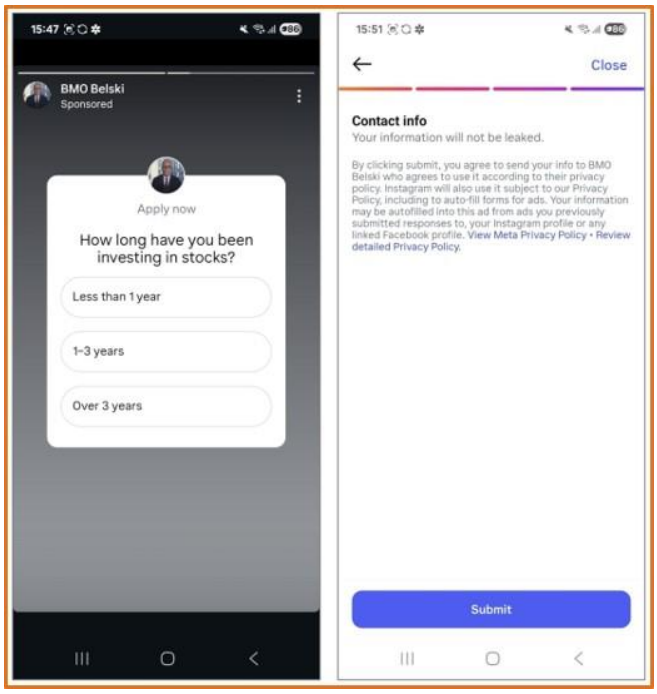

Figure 8 - 'BMO Belski' campaign's Instagram Story and Poll.

The 'BMO Belski' campaign also produced relatively convincing deepfake videos (safe Vimeo link) of Brian Belski for the same purpose of driving users into joining the scam WhatsApp group.

Figure 9 - Video deepfake of Brian Belski advocating for scam WhatsApp group.

Recommendations

These recent fraudulent ad campaigns demonstrate the persistent nature of online scams and their constant evolution in line with developing technologies such as generative AI. The following recommendations are provided to help combat similar scams:

- Online users must exercise heightened caution when encountering unsolicited offers on social media platforms, especially those delivered through ads or designed to imitate legitimate communications or services.
  - Remain vigilant to the potential use of audio deepfakes impersonating executives, particularly those with significant public exposure, as this provides ample material to produce highly convincing forgeries.
  - Indicators such as mismatched domain names, or newly created pages or accounts impersonating well-established brands remain helpful red flags.
- Organizations should utilize the findings in this report to update user awareness training programs, ensuring they reflect the latest tactics, techniques, and trends in online scam campaigns.
- Enable Multi-Factor Authentication (MFA) wherever possible to minimize the effect of fraudulent ad campaigns targeting credentials
- Network defenders are advised to block the IOCs provided below.

Indicators of Compromise

Network Indicators	Further Detail
`47.239.216[.]183`	Impersonating GoA
`albertagov[.]ca`	
`ccr-alberta[.]com`	
`ccr-alberta[.]info`	
`myalbertaccr[.]ca`	
`sellmyhouseinalberta[.]com`	Other domains impersonating Alberta-based assets registered through NameSilo
`rimeyalberta[.]ca`	
`albertawebsite[.]ca`	
`albertaheatlthservices[.]ca`	

92.53.111[.]163	Impersonating Red Deer MyRide
startlight-ventures[.]com	
mindfultech[.]live	Investment scam impersonating CBC News
rbcpromos1[.]cfd	Fraudulent ads impersonating Canadian banks