Smishing Campaign Impersonating the Government of Alberta

This report is distributed as **TLP:CLEAR**. Recipients may share this information without restriction. Information is subject to standard copyright rules.

Disclaimer | CyberAlberta

Summary

On 26 November 2025, the Government of Alberta (GoA) and CyberAlberta Threat Intelligence identified a SMS phishing (smishing) campaign targeting Albertans. Further analysis revealed similar campaigns impersonating government and private services across Canada.

Details

On 26 November 2025, Service Alberta and Red Tape Reduction (SARTR) received multiple reports from Albertans of a suspicious SMS message regarding a vehicle registration refund (Figure 1). Specifically, the SMS message alleges a refund on their 2024 vehicle registration and directs the user to a URL to view the status of their refund.

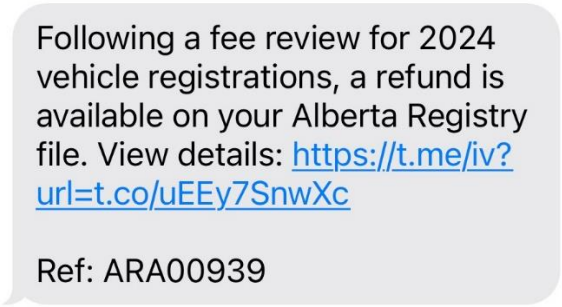

Figure 1. Smishing text message received by users

If the victim visits the provided link, the following occurs:

1. The user is taken to a Telegram page with a secondary link (Figure 2).

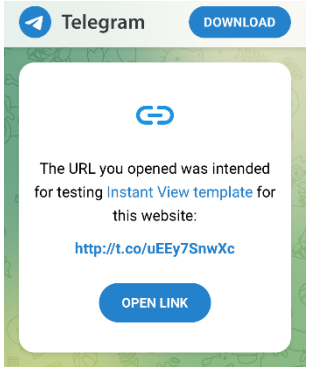

Figure 2. Telegram Redirect

2. After clicking on the secondary link, the user is then taken to `alberta-rfnd24[.]com` where they are presented with a GoA-themed CAPTCHA to gain access to the site (Figure 3).

Figure 3. GoA-themed CAPTCHA Page

3. Once the CAPTCHA is verified, the user is informed they have a $25 credit for their 2024 vehicle registration. The spoofed site appears convincing, featuring an image of Alberta's new license plate officially revealed on 18 November 2025. If the user continues through the chain, the last form requests their financial information (Figure 4).

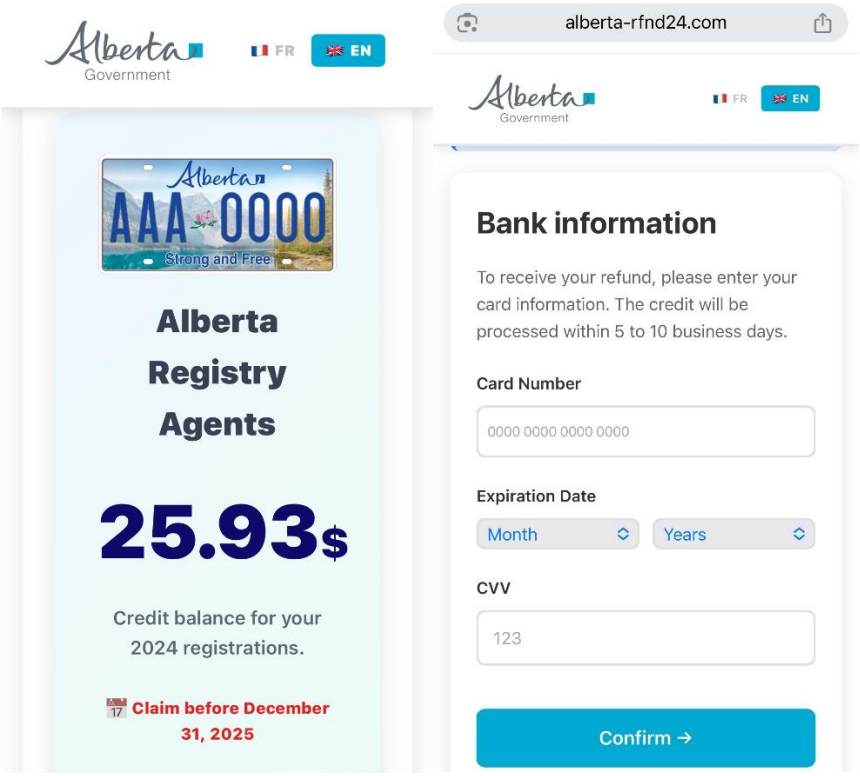

Figure 4. Spoofed GoA Registration Site

Connected Infrastructure

Analysis of this campaign's infrastructure revealed several domains established to impersonate other services, such as government, utility companies, and transport organizations. All identified impersonating domains are provided in the Indicators of Compromise (IOCs) section below.

Assessment

This campaign is similar to multiple campaigns previously analyzed by CyberAlberta Threat Intelligence in June 2025.[1] This continued targeting of localized audiences likely increases the campaign's appearance of legitimacy. Users must be vigilant when receiving unsolicited messages claiming to offer financial awards.

Recommendations

- Do not engage with any suspicious messages which appear to contain fraudulent links. Instead, report the messages using the appropriate reporting mechanism for your device, or to the RCMP Report Cybercrime & Fraud service[2].
- Verify all sources related to monetary actions. Sources that claim refunds or money owed should be verified and followed through using official channels and means of communication.

Indicators of Compromise (IOCs)

The following IOCs characterize the activity described in this report.

Description	Indicator
IP used to host impersonating domains	104.168.101[.]24
Domains impersonating government services	407etr-notice[.]xyz
	alberta-rfnd24[.]com
	alberta-rfnd25[.]com
	revenue-qc093[.]com
	rfnd-quebec[.]xyz
	saaqclic-notification[.]xyz
	sgi-rfnd24[.]com
	novascotia-rfnd24[.]com
Domains impersonating utility companies	bchydro-rfnd03[.]com
	bchydro-rfnd93[.]com
	bchydro-rfnd24[.]com
	hydroqc-32093[.]com
	hydroqcnotif23[.]xyz

[1] https://cyberalberta.ca/fraudulent-ads-on-social-media-target-national-and-local-users
[2] https://reportcyberandfraud.canada.ca/

	2024-hydroqc[.]com
Domains impersonating shipping companies	test-check-route[.]xyz
	notification-so[.]xyz
	asjksakjl32[.]xyz
	asjhklias32[.]xyz
	dnspod412[.]com

Table 1. Indicators of Compromise