THREAT REPORT: GoA SMS Phishing Scam & Spoofed Website

March 22, 2024

TLP: WHITE

Source: **CyberAlberta Community of Interest Member**

UPDATE:

It has come to light that there is another spoofed webpage running an identical phishing campaign. The new impersonating domain is **infractions-ab[.]com**. The GoA is taking action to also have this site removed.

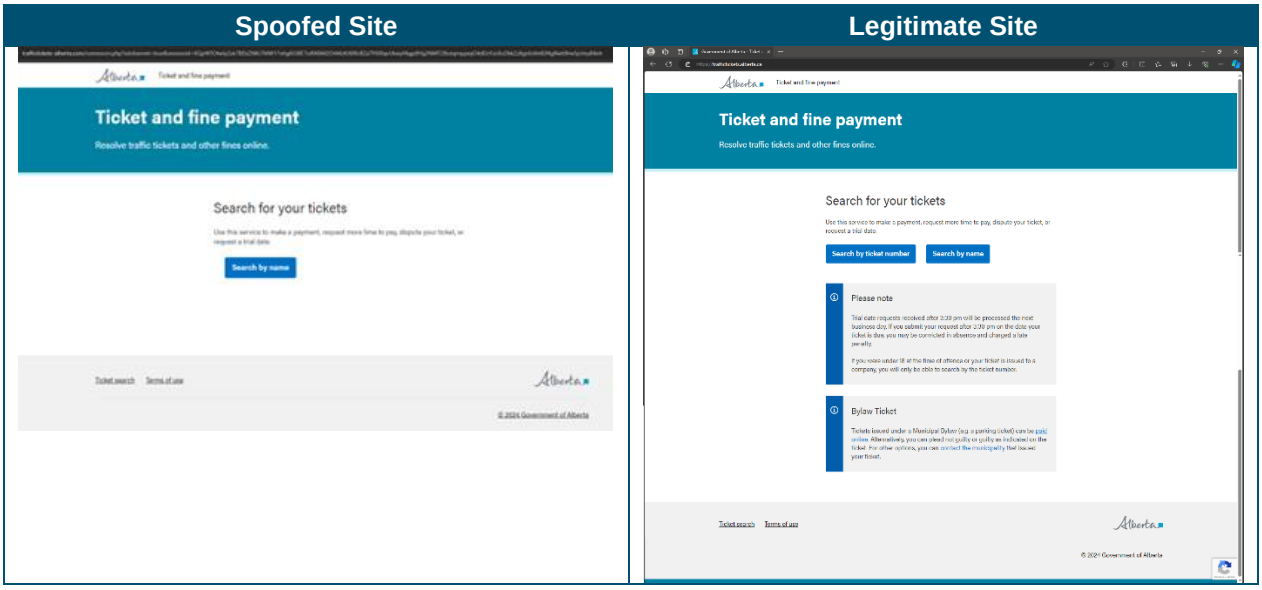
Overview:

On 16 March 2024, CyberAlberta Community of Interest member reported a SMS message received indicating that the recipient had been caught speeding and requested the user click a link to address the ticket:

An open-source search shows that this is not a unique message and that other Albertans have received similar messages recently. The site that is linked to appears legitimate at first glance, including approximating Government of Alberta (GoA) branding, which could lead to confusion if Albertans are not aware that speeding notifications are always mailed and not texted.
If the recipient clicks the link the following occurs:

1. The user is taken to **trafficticketsalberta[.]com** where they face a CAPTCHA to gain access.
    - NOTE: The legitimate site for addressing speeding tickets is **trafficticketsalberta.ca**

2. Once the CAPTCHA is completed, access is granted to the site. The site is a believable spoof of the legitimate GoA Ticket and Fine Payment site:



- NOTE: Original reporter has noted and the GoA Threat Intel team has confirmed that the IP address for this website is Russian affiliated (RIPE) (VirusTotal) (Cisco Talos) (URLScan). Please note this does not necessarily indicate that a Russian-affiliated threat actor is responsible.

3. If the recipient clicks further into the website, they will be met with legitimate appearing forms first requesting basic personally identifiable information (e.g., name, date of birth, phone number, address, email).

4. Regardless of the information provided in this form the recipient will be informed they have an outstanding payment due and be pointed towards a payment link in order to avoid a court appearance.

5. If the user clicks the payment link, they will be directed towards a second form requesting credit card information.

What to Communicate to Executives:

- **GoA Action:** GoA has taken action into having this spoofed website removed as it is clearly attempting to phish information from Albertans. The information has also been shared on X (formerly Twitter) by the Service Alberta and Red Tape Reduction Team to increase awareness with Albertans.

- **Verify Source:** If a link appears to be received from a trusted source, validate that this link is legitimate using other means (e.g., look to information you know is legitimate for confirmation of the link, confirm via a phone call, email, etc. that the link is real). All links regardless of source should be treated with skepticism until you can verify them, and if they cannot be verified or something appears off, they should not be engaged with.

- **Report:** Any suspicious messages which appear to contain a fraudulent link should be reported using the appropriate reporting metric for the avenue received (e.g., SMS reporting, phishing

reporting, etc.). If you suspect that there is a spoofed website, reach out to the appropriate organization to inform them that their website is being impersonated.

Further Reading:

- Phishing - Top 10 Best Practices | CyberAlberta
- Don't take the bait: Recognize and avoid phishing attacks | Canadian Centre for Cyber Security
- Real examples of fake online stores | Get Cyber Safe