



RGSA 04-25-24-01
Date: April 25, 2024

SMS Phishing Scams Targeting Road Toll Payments

INTRODUCTION

A wave of SMS phishing attacks targeting Canadians with lures regarding unpaid road toll fees have been rolling out since the beginning of the year. 407 ETR has been warning customers to beware of fraudulent texts impersonating the company. The message is designed to deceive people into clicking on a malicious link, which would leave people vulnerable to personal data theft.

HOW TO TELL IF A 407 ETR MESSAGE IS LEGITIMATE

407 ETR will use specific communication methods to interact with customers that use the express toll route. If you are a customer that uses the 407, take note of these legitimate communication channels:

- 407 ETR sends payment reminder text messages from a six-digit short code. Messages don't contain any personal or account information and include a link to their secure payment web page. Their texts will never include a direct link to pay.
- 407 ETR makes outbound automated payment reminder calls. These calls will not ask you for your personal information.
- 407 ETR will only send emails from info@407etr.com or communications@407etr.com. Ensure that the emails you receive do not have spelling errors.

HOW RICHTER GUARDIAN CAN HELP YOU

- Call us or send us an email at: +1 844-908-3950 and support@richterguardian.com if you are unsure. Connect with our cyber concierge to verify the legitimacy of a situation.
- Transunion identity protection is included on our platform. Transunion identity protection will alert you of any unusual activity on your credit monitoring report that could indicate fraud.

CONTACT US



Have a quick question? Send us an email.
Email: support@richterguardian.com



Phone number: +1 844.908.3950
Monday to Friday 9 a.m. to 5 p.m. (Eastern Time)



Need assistance upgrading your device?
Schedule a session with us by clicking [here](#)