BEEP, BEEP - SCAM AHEAD!

Don't Let Fake Toll Texts Derail Your Summer Road Trip

Office of Information Technology
Division of Information Security

JUNE 2025

As summer travel ramps up, unfortunately, so do the scams, and one of the latest hitting drivers is fake toll road text message scams. These phishing messages often look legitimate, claiming you owe unpaid tolls and prompting you to click a link to resolve the issue. The scam can be used to steal both the victim's personal information and their payment details, and allows cybercriminals to add victims' credit cards to an Apple or Google wallet.

The toll road scam is effective because it often requests a small payment, making the request appear reasonable. However, clicking the link can result in identity theft, stolen credit card information, or malware infecting your device.

If you recently received a text message claiming you owe money for unpaid tolls, you are not alone. According to the FBI's Internet Crime Complaint Center, they have received thousands of reports of this scam. Here is some information to help protect you and your wallet.

How does this Scam Work?

Scammers send a text message that appears to be from a legitimate toll agency. The messages often claim that you have an overdue toll charge and that you must pay immediately to avoid fines or license suspension. Although the details of each scam or text message can differ, many users have reported that scammers are frequently:

- **Using the Toll agency's full name.**
- **Alleging that the user owes an unpaid toll and warning of potential legal consequences.**
- **Demanding that the fine be paid quickly.**
- **Including a link in the text message with a "gov" in it.**

The link in the message usually leads to a website that looks like a real toll agency website. The users are prompted to enter sensitive information such as their name, address, license plate number, credit card details, and even their Social Security number.

DMV Final Reminder:
You have an outstanding toll.Your toll account balance is outstanding. If you fail to pay by July 11, 2025. You will be penalized or subject to legal action.

Please reply Y to begin payment.

You must settle your toll immediately after reading this message to avoid penalties for delaying the payment.

Thank you for your cooperation.

These scams are successful because they can appear at just the right moment, such as right after a road trip or your daily workday commute. Scammers rely on urgency, familiarity, and professional-looking government websites.

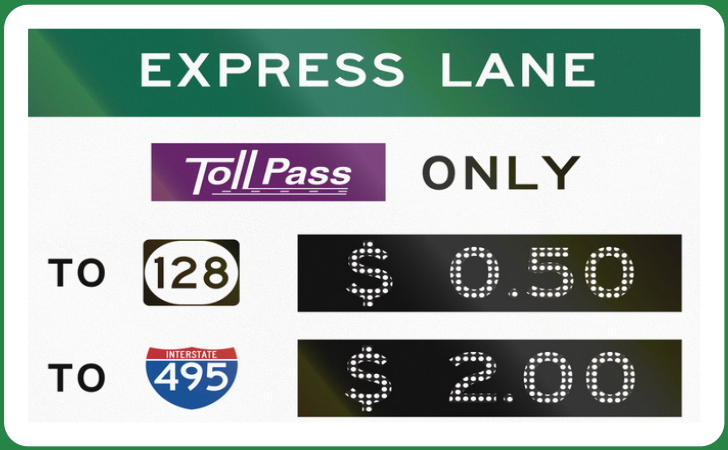
Here is what to look out for:

- Unexpected messages from toll agencies
- Spelling errors or bad grammar
- Generic greetings such as “Dear customer” instead of using your name
- Suspicious links
- Demands for immediate payments or threats of fines.

How to Protect Yourself

- Do not click links in unsolicited text messages.
- If you receive a suspicious text message, you can verify the message by logging into your toll account directly through the official website.
- Call customer service directly if you have questions about your account.
- Report and delete unwanted text messages. Use your phone’s “report junk” option to report unwanted texts to your messaging app or forward them to 7726 (SPAM). Once you’ve checked it out and reported it, delete the text.
- Check your bank and credit card activity for unauthorized charges.

If you have accidentally provided a payment, contact your bank or credit card provider immediately, and update any compromised passwords. You can also report suspicious messages and scams to the Federal Trade Commission. If you believe your personal or financial information has been exposed, such as a credit card, bank account number, or other sensitive details, visit IdentityTheft.gov. This site provides step-by-step instructions, including how to report the issue to your bank or credit card company and how to cancel your credit card.



A secure and scam-free summer begins with awareness. By staying informed and alert, you can protect your personal information and enjoy your summer travels.

NOTE: *The links in this document are for informational purposes only, and do not signify an endorsement of any products contained within the linked sites/files.*

Please contact cybersecurity@ihs.gov with any questions or comments about this newsletter.