THREAT BULLETIN

AR20250609-28 [Advisory Report] Maryland Residents Receiving Fake Traffic Citation/Violation Smishing Messages Impersonating MDOT MVA

TLP
Clear

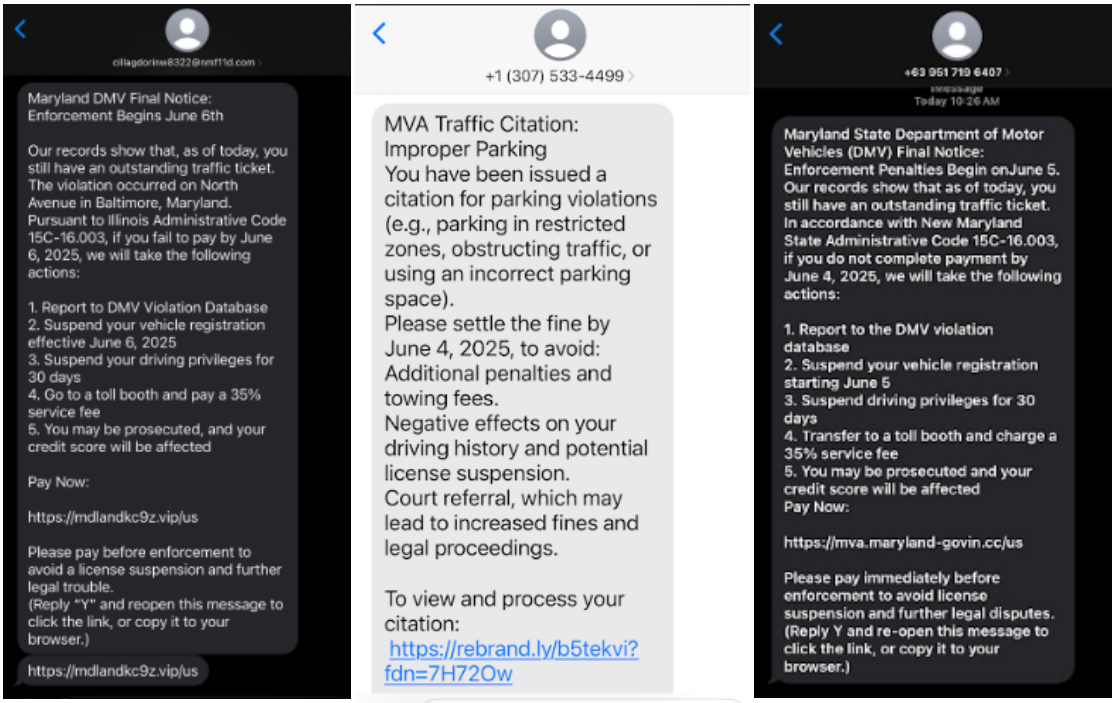
DESCRIPTION

AR20250609-28 [Advisory Report] Maryland Residents Receiving Fake Traffic Citation/Violation Smishing Messages Impersonating MDOT MVA

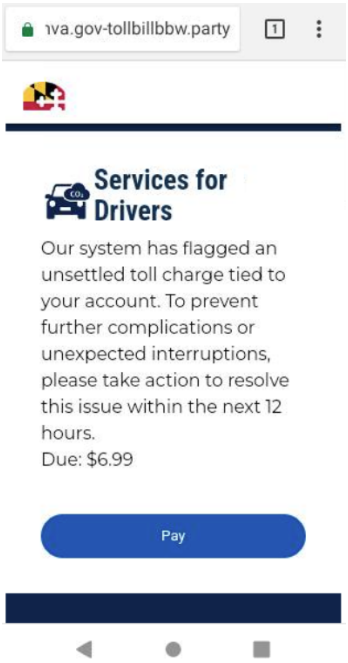
TLP:CLEAR = Recipients can spread this to the world, there is no limit on disclosure

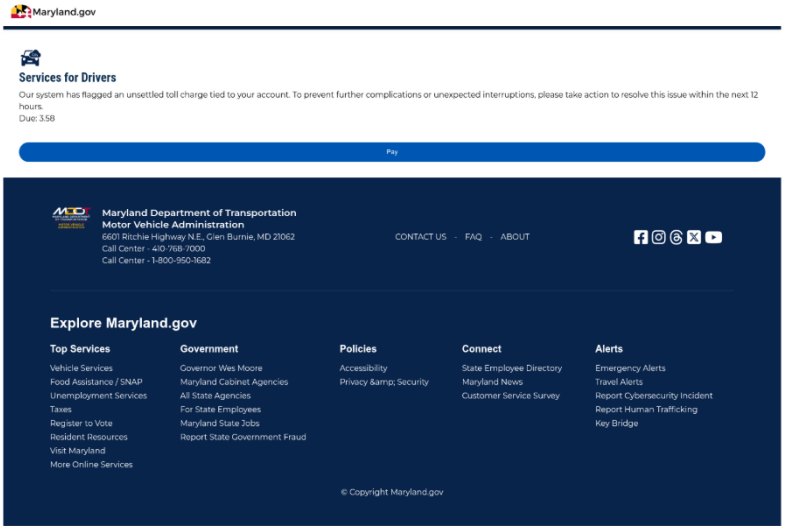
Summary

Another smishing campaign has been observed targeting Maryland vehicle owners claiming to be the Maryland Motor Vehicle Administration informing residents they must complete payment for a traffic violation before they are charged an additional fee. The links in the message are typosquats or look-alike domains that aim to harvest information and/or credentials from victims. This activity follows a recent similar campaign targeted at EZpass users and is consistent with a widespread trend across many states reporting high volumes of automotive-related smishing messages.



Sample smishing messages received by Maryland residents. When clicking on the link lead to the following impersonation pages (shown on mobile and desktop view):





The MD-ISAC advises all Maryland residents to complete all traffic violation payments through the official payment links found at https://mva.maryland.gov/ and to report any suspicious messages to the MD-SOC at mdsoc@maryland.gov or (410) 697-9700 - option #5.

Reporting and Contact Information

In the event of a cybersecurity incident related to information found in this threat bulletin, Md. Code, Public Safety Article § 14-104.1 (c)(2) and Md. Code, State Finance & Procurement Article § 3.5-406(b)(2)) mandate that you report this via the Maryland Incident Reporting System. It is also recommended that you submit any shareable cyber threat intelligence to the MD-ISAC via the MD-ISAC Threat Intelligence Platform (TIP).

TLP:CLEAR = Recipients can spread this to the world, there is no limit on disclosure

TLP:CLEAR = Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information about Traffic Light Protocol (TLP) definitions and usage: https://www.cisa.gov/tlp