MD-ISAC
Maryland Information Sharing and Analysis Center

POWERED BY ANOMALI

THREAT BULLETIN

AR20241016-33 Maryland Residents Receiving Smishing Messages Impersonating MDOT EZ-Pass

TLP
Clear

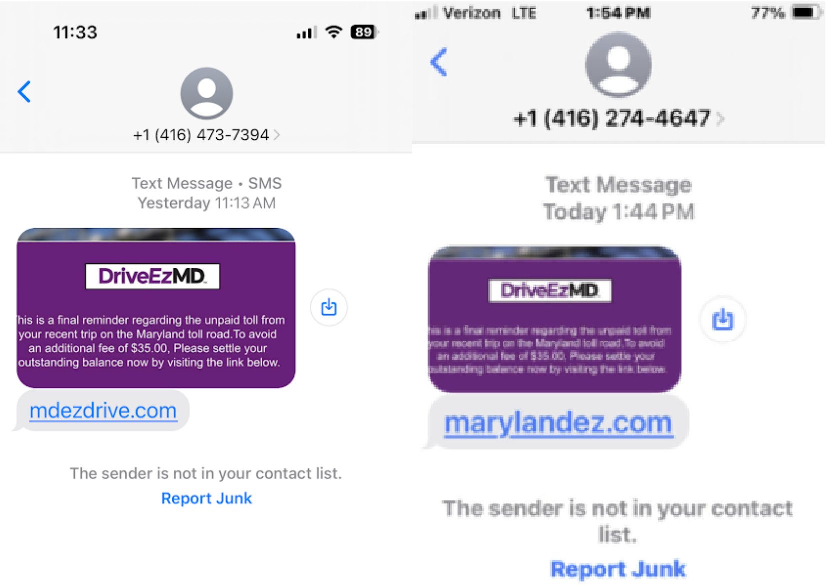
DESCRIPTION

Maryland Residents Receiving Smishing Messages Impersonating MDOT EZ-Pass

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

Summary

Multiple Maryland residents have reported receiving SMS phishing (smishing) messages claiming to be the Maryland Department of Transportation - Maryland Transportation Authority informing them that they must complete payment for an unpaid toll 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 trend present in many other states, which all report high levels of toll related smishing messages.



11:33

+1 (416) 473-7394

Text Message • SMS
Yesterday 11:13 AM

DriveEzMD

his is a final reminder regarding the unpaid toll from your recent trip on the Maryland toll road.To avoid an additional fee of $35.00, Please settle your outstanding balance now by visiting the link below.

mdezdrive.com

The sender is not in your contact list.
Report Junk

Verizon LTE 1:54 PM 77%

+1 (416) 274-4647

Text Message
Today 1:44 PM

DriveEzMD

his is a final reminder regarding the unpaid toll from your recent trip on the Maryland toll road.To avoid an additional fee of $35.00, Please settle your outstanding balance now by visiting the link below.

marylandez.com

The sender is not in your contact list.
Report Junk

Sample smishing messages recieved by Maryland residents

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

Incident Response

If administrators discover signs of attack or system compromise, the MD-ISAC recommends they:

- Consider soliciting support from a third-party incident response organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
- Report incidents to MD-ISAC via Maryland's 24/7 Operations Center (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