NEW YORK STATE SENATOR

John J. Flanagan

DMV Warns Consumers of Fake Ticket Email Hoax Meant to Collect Personal Information

JOHN J. FLANAGAN June 2, 2017

ISSUE: DMV (DEPARTMENT OF MOTOR VEHICLES)

The New York State Department of Motor Vehicles (DMV) is cautioning consumers against an email "phishing" campaign that sends a notice to email users stating they must pay a ticket within 48 hours or their license will be revoked. While the notice is made to appear as if it comes from DMV, it is a hoax.

The fake emails pretend to be from DMV, and report that the State Police has advised DMV that the recipient has several outstanding traffic violations. It then provides two links to either plead guilty or to refute the tickets. The links direct unsuspecting users to a malicious

download that may expose your computer to a virus. If you receive one of these emails, delete the email immediately. Do not click on any links in the email and do not forward the email.

“The Department of Motor Vehicles does not send emails urging motorists to pay traffic tickets within 48 hours or lose your license,” said Terri Egan, DMV Deputy Executive Commissioner. “It is unfortunate that people use our agency’s name to target innocent consumers. We urge New Yorkers to always remain cautious about opening email attachments or following links, even if they appear to come from legitimate agencies.”

“With the rise in the use of the Internet and mobile devices to conduct everyday business, there is also an increase in the frequency of email scams and phishing incidents. The Office of Information Technology Services urges New Yorkers to always treat emails containing links or attachments with caution. Phishing emails can be difficult to identify, however being aware of the threat and being vigilant in examining emails can reduce the risk that you will fall prey to such an attack,” said Robert H. Samson, New York State Chief Information Officer.

The following tips can help mitigate a phishing attempt and keep your personal data safe:

- Exercise caution with all email communications you receive, including those that purport to be from a trusted entity. Inspect the sender’s information to confirm the email was generated from a legitimate source.
- Keep an eye out for telltale signs of phishing - poor spelling or grammar, the use of threats, the URL does not match that of the legitimate site. If the message does not feel right, chances are, it is not.
- Be suspicious of links embedded in an unsolicited email.

- Don’t open unexpected email attachments. The attached files may be hiding malicious software.
- Don’t send your personal information via email. Legitimate businesses will not ask users to send sensitive personal information through email.
- Don’t post sensitive information online. The less information you post, the less data you make available to a cybercriminal for use in developing a potential attack or scam.
- Use strong passwords – Use a combination of upper- and lower-case letters as well as numbers and symbols when creating a new password. Don’t use your name, birthdate, or common words. Use a different password for each of your accounts.

A similar hoax occurred in 2011 when people received an email that purported to be a Uniform Traffic Ticket from DMV. That hoax included an attached zip file, which recipients were led to believe was a copy of the ticket, but planted a virus when opened.

If you do open such an attachment or click such a link, you should immediately update and run your antivirus software and take steps to be sure your computer system is secure. Do not forward the email to State Police or local law enforcement but do alert them.

This hoax email lists a reference number then reads in part:

“Dear Driver:

We are writing to inform you that the state police department has notified us that you have several outstanding traffic violations. If you do not make restitution for these infractions within 48 hours, we will be forced to revoke your driver’s license.

To make payment arrangements online, click here.

To refute these tickets, click here.

Sincerely,
The NY DMV”

“At no time do we send the type of email described in this hoax,” Egan said. “While DMV does include links in many of the emails we send, the links always lead to a page on a state-affiliated website.”

The phone numbers for the DMV call centers can be found on the DMV website. You can email us through the Ask DMV a Question service. Report suspected Phishing scams to spam@uce.gov, to the Division of Consumer Protection, and to the institution or company targeted in the Phishing e-mail. You also may report Phishing e-mails to the Anti -Phishing Working Group at reportphishing@antiphishing.org.