PENNSYLVANIA STATE POLICE

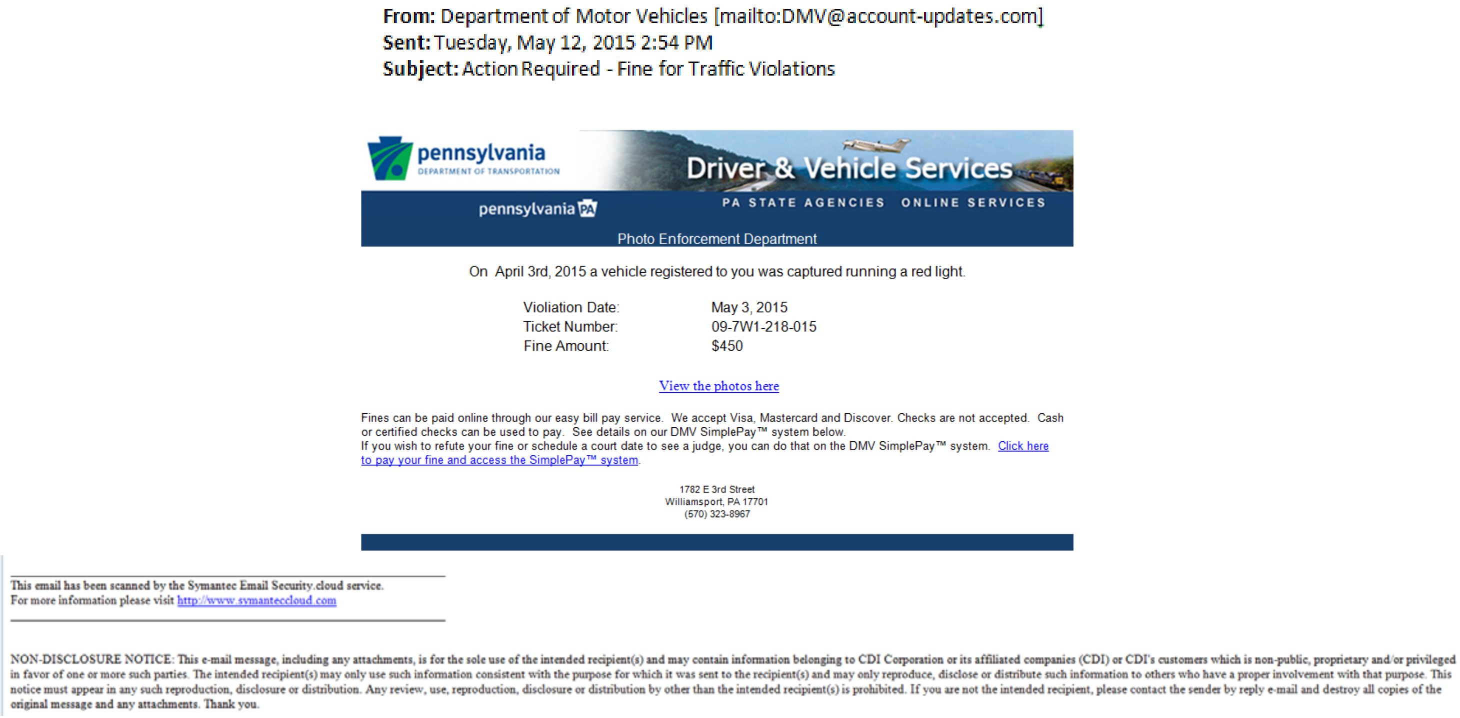
COMMUNITY AWARENESS BULLETIN

CAB 003-15 May 14, 2015

PHISHING EMAIL ALERT

The Pennsylvania Criminal Intelligence Center (PaCIC) has recently received information regarding a fraudulent email claiming to originate from the Pennsylvania Department of Motor Vehicles (PennDOT). The subject line of the email indicates “Action Required - Fine for Traffic Violations.” The body of the email further states that “a vehicle registered to you was captured running a red light” along with a violation date, ticket number, and a specified fine amount. There were also various links to click on to view photos, pay the fine, or for more information regarding the email security service. These links redirect the user to other websites not affiliated with PennDOT.

Below is an example of the actual email received as part of this particular scam. There are signs that indicate this is a phishing scam, including: poor spelling or grammar within the message. This message not only has “violation” spelled incorrectly, but also lists two different violation dates. Additionally, citations or traffic tickets issued in Pennsylvania are not paid directly to PennDOT.


pennsylvania
DEPARTMENT OF TRANSPORTATION
Driver & Vehicle Services
pennsylvania PA
PA STATE AGENCIES ONLINE SERVICES

From: Department of Motor Vehicles [mailto:DMV@account-updates.com]
Sent: Tuesday, May 12, 2015 2:54 PM
Subject: Action Required - Fine for Traffic Violations

Photo Enforcement Department

On April 3rd, 2015 a vehicle registered to you was captured running a red light.

Violiation Date:	May 3, 2015
Ticket Number:	09-7W1-218-015
Fine Amount:	$450

View the photos here

Fines can be paid online through our easy bill pay service. We accept Visa, Mastercard and Discover. Checks are not accepted. Cash or certified checks can be used to pay. See details on our DMV SimplePay™ system below.
If you wish to refute your fine or schedule a court date to see a judge, you can do that on the DMV SimplePay™ system. Click here to pay your fine and access the SimplePay™ system.

1782 E 3rd Street
Williamsport, PA 17701
(570) 323-8967

This email has been scanned by the Symantec Email Security.cloud service.
For more information please visit http://www.symanteccloud.com

NON-DISCLOSURE NOTICE: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain information belonging to CDI Corporation or its affiliated companies (CDI) or CDI's customers which is non-public, proprietary and/or privileged in favor of one or more such parties. The intended recipient(s) may only use such information consistent with the purpose for which it was sent to the recipient(s) and may only reproduce, disclose or distribute such information to others who have a proper involvement with that purpose. This notice must appear in any such reproduction, disclosure or distribution. Any review, use, reproduction, disclosure or distribution by other than the intended recipient(s) is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message and any attachments. Thank you.

Fraudulent emails purporting to be from legitimate government agencies is not new, but such scams often change form. Phishing is the process of deceiving recipients into sharing sensitive information with an unknown third-party, or cyber attacker, typically through email; however, websites and internet pop-up ads are also used.[1] When using email, it is difficult to know exactly with whom you are communicating. Scammers utilize this uncertainty to pose as legitimate businesses, organizations, or individuals to gain the trust of users and compromise their personal, financial, and/or other sensitive information. Scammers appear to represent legitimate businesses or organizations by spoofing email addresses, creating fake websites with legitimate logos, and providing phone numbers to illegitimate customer service centers or tech support centers operated by attackers.

Recommendations

- ***Follow Best Practices.*** Please make sure users follow best security practices regarding email security. Do not reply to these types of emails and delete the message if and when received. If you receive an email asking for privileged information, you should delete it immediately.
- ***Never give out privileged information.*** Oftentimes "Phishing" emails will use legitimate 'From:' email addresses, well-known logos, or links to reputable businesses in the message. Some may ask for personal information such as your name, address, date of birth, Social Security number (SSN) passwords etc. You should never reply to inquiries asking for privileged information. If you do receive these types of requests through email or via verbal request, please do not reply to the request.
- ***Don't open anything from an unknown source.*** If the sender's name is not recognized, it should not be opened. If the name is recognized, but the contents appear questionable, contact that person to verify they sent the email. Always remember not to click on links or attachments contained in e-mails from un-trusted or unknown sources.
- ***Remember that it always pays to be careful.*** If it looks suspicious or if there is a doubt about its legitimacy in any way, delete the message and do not reply or ask your IT department for assistance.

Always remember the following cyber security tips when dealing with content and links in suspicious e-mails:

- **NEVER** open a link or attachment when the sender is not known.
- **NEVER** click on an e-mail link that only has an IP address.
- **NEVER** run a program or allow a plug-in when the source is unknown or un-trusted

[1] Cyber crime: A technical desk reference. (2013). Center *for Internet Security*. Retrieved 05/13/2015.
[2] DuPaul, N. (n.d.). Spooking attack: IP, dns & arp. *Veracode.* Retrieved 05/13/2015 http://www.veracode.com/security/spoofing-attack.