July 1, 2021

*****CONSUMER ALERT*****

ATTORNEY GENERAL RAOUL URGES ILLINOIS RESIDENTS TO BE ALERT FOR TEXT PHISHING OR 'SMISHING' SCAMS

Individuals Should Be Wary of Texts from People Claiming to Work for State Agencies

Chicago — Attorney General Kwame Raoul today urged Illinois residents to be alert for text messages from individuals claiming to represent state government agencies. Raoul's office is warning that the unsolicited messages may be SMS phishing, or "smishing" scams, and people should delete and not open links or respond to such texts.

The Attorney General's office is warning of increased instances of people receiving unsolicited text messages from individuals claiming to represent the Illinois Secretary of State's office and the Illinois Department of Transportation (IDOT). Texts inform recipients they must validate their driver's license information by clicking on a link provided in the message.

"People should know that government agencies will not request sensitive personal information via unsolicited text messages," Raoul said. "If you receive such a message – even if the phone number appears to be local – do not respond. If you are unsure about whether the request is legitimate, contact the agency in question using information from the agency's official website."

Attorney General Raoul cautions people against assuming a text is legitimate just because it comes from a familiar phone number or area code. Scammers use caller ID spoofing in smishing text scams to make it appear as though the text is from a reliable source so they can convince recipients to provide personal information, click links that will install malware on recipients' devices, or direct recipients to click on a web link that will take them to a spoofed website. If recipients attempt to enter usernames and passwords to access the fake websites, that will allow scammers to access or steal information.

Raoul stresses that government agencies will not send unsolicited text messages requesting driver's license numbers or other sensitive information. Raoul encourages consumers to take the following steps to protect themselves from text scams or smishing:

- **Do not share your phone number** unless you are sharing it with a person or organization you know well. Use caution when providing your cellphone number or other information in response to pop-up advertisements and "free trial" offers. This personal information can be easily bought, sold, and traded, and make you a target for smishing scams.
- **Do not act immediately.** Smishing scams attempt to create a false sense of urgency by implying that an immediate response is required, or that there is a limited time to respond. Take time to verify the sender's identity, and ask yourself why the sender is asking for your information.
- **Keep software up to date,** including on cellphones, to help avoid viruses placed by scammers.

People can report smishing texts to their cellphone carriers by copying the original text and forwarding it to 7726 (SPAM), free of charge. Individuals also can report scam texts by visiting the Federal Communications Commission's website or by calling 888-225-5322. Additionally, there are steps people should take if they have replied to smishing texts or clicked on links provided in such texts. Raoul urges those individuals to do the following to reduce the risk of identity theft:

- **Run a full virus/malware check** on your device after ensuring all antivirus/antimalware scanning software is updated.
- **Consider placing a fraud alert** on your credit report by contacting one of the three major consumer reporting agencies: TransUnion, Equifax or Experian. Fraud alerts act as a red flag to potential creditors signaling that they should ask for additional information to verify your identity. Fraud alerts last for one year and do not impact your credit report or the credit score derived from data within your credit report.
- **Consider freezing (or placing a security freeze on)** your credit reports. You must contact all three major consumer reporting agencies separately to request a freeze. Credit freezes are free to place and lift and do not impact your credit score, but they must be lifted in order for you to apply for credit or a loan.
- **Review your credit reports,** and promptly dispute any inaccurate entries with both the consumer reporting agency and the creditor. Go to annualcreditreport.com or call 1-877-322-8228 to receive your free credit reports.
- **View your financial account statements** at least once a month, if not more frequently, and promptly dispute any unauthorized transactions with your bank.
- **Place transaction alerts with your bank** by requesting notification when more than a preset amount of your choosing is charged to your account. Transaction alerts can be configured to provide text message and/or email message alerts. If you receive notice of a transaction that you did not initiate, you should dispute it immediately with your bank.
- **Practice good password hygiene:** change your passwords on a regular basis, and don't reuse passwords; create strong passwords using multiple character variations; consider implementing two-factor authentication for account access; and create different passwords for different websites and account logins.

Attorney General Raoul encourages people who have questions about protecting against identity theft and setting up credit monitoring to call the Illinois Attorney General's Identity Theft Hotline at 1-866-999-5630 to speak to a specially-trained advocate.