Attorney General Raoul Urges Illinois Residents To Be Alert For Email And Text Message Scams

June 7 2023 10:39 AM

CHICAGO - Attorney General Kwame Raoul today urged Illinois residents to be wary of scammers who use unsolicited email or text messages to trick consumers into sharing personal and financial information. Raoul encourages all consumers to stay aware of these unsolicited messages and to continue to report these incidents to his office.

Unsolicited messages may be email phishing or text message smishing scams. Phishing is when scammers send a deceptive email to trick Internet users into revealing personal or confidential information. Smishing, or Short Message Service (SMS) phishing, is when scammers send a deceptive text message to trick cell phone users in the same way.

Phishing and smishing messages may contain links to harmful software that could enable scammers to steal information from your phone or computer. Raoul's office warned consumers to not click any links in an unsolicited email or text and to delete the message immediately.

"Consumers should be suspicious of unsolicited emails and text messages asking for personal or financial information. It is important to know government agencies will not request sensitive personal information via an email or text message," Raoul said. "Even if a phone number appears to be local or an email address seems familiar, do not respond. If you think a message is suspicious, contact the business or agency in question using information from its official website."

Raoul also offered the following tips to help consumers protect themselves from scammers:

- **Do not share your phone number or other personal or financial information.** Do not give out your Social Security number, bank routing numbers, or other personally-identifiable financial information unless you know who you are providing it to and why. Use caution when providing a cell phone number or other information in response to pop-up advertisements or free trial offers. This personal information can be easily bought, sold and traded for smishing scams.
- **Beware of suspicious contacts.** Government agencies will not call, email or text to ask for money or personal information. If you receive a suspicious correspondence, search for the business or agency's official website, and call the number listed. Keep in mind that government agency website addresses typically end in .gov or . org.
- **Do not act immediately.** Smishing scammers attempt to create a false sense of urgency by implying an immediate response is required or that there is a limited time to respond. Take time to verify the sender's identity, and ask why the sender is asking for personal information.
- **Never open a link or an attachment from unsolicited, suspicious or unexpected text or email messages.** Scammers can use a variety of tactics to hack email or social media accounts once you click a link or open an attachment. These actions can also lead to malware being downloaded onto your cell phone or computer.
- **Do not respond to suspicious text messages, even to say "STOP."** Replying to smishing messages verifies a phone number is active and willing to open such messages, which may lead to more unsolicited text messages.
- **Report phishing emails or smishing text messages.** Call the Attorney General's office or file a consumer complaint with the Illinois Attorney General's office. Report phishing or smishing messages to the Federal Communications Commission

online or by calling 888-225-5322. You can also report smishing texts to your cellphone carrier by copying the original text and forwarding it to 7726 (SPAM), free of charge. Promptly block the senders and delete all messages after reporting.

Raoul advised those who have replied to smishing texts or clicked on links provided in such texts and emails can reduce the risk of identity theft by signing up for free bank or credit card transaction alerts, placing a fraud alert with one of the three credit reporting agencies, or placing a freeze on their credit reports. Those individuals also should update their computer's security software, run a scan and remove anything identified as a problem. Consumers should also make sure they are using the most updated version of their phone's operating system.

If you believe you have been the victim of identity theft or other fraud, Raoul encourages you to file a complaint on the Attorney General's website, review the identity theft online resources and call Raoul's toll-free Identity Theft Hotline at 866-999-5630. Consumers can also call one of the Attorney General's Consumer Fraud Hotlines:

1-800-386-5438 (Chicago)
1-800-243-0618 (Springfield)
1-800-243-0607 (Carbondale)
1-866-310-8398 (Spanish-language hotline)