Retired State Employees Association
P.O. Box 1974
Springfield, IL 62705-1974
www.RSEA4U.org

The Retired State Employees Association (RSEA) would like to inform our members and all other seniors that there have been a series of fraud attempts recently.

The State Employees Retirement System (SERS) recently notified retirees that there are MANY fraudulent attempts being sent through texts and emails **pretending to be SERS**. SERS will **NEVER** text retirees asking for personal or financial information. While some emails may appear to be legitimate because they contain the SERS logo - ALL legitimate emails from SERS will come from an account ending in **@srs.illinois.gov**. If the text or email promises you payment of your monthly benefit early, **it is a scam** – there is no such program. The scammers have partially copied a SERS document to make you think it is possible and that they are SERS. Some of the scam emails reference a popular application called "DocuSign." Please know that – SERS **DOES NOT** utilize this application for any direct deposit changes, nor do they ask for electronic signatures! **SERS does not accept digital signatures, only signatures made with an ink pen on paper forms they provide to you!**

With the recent data breaches/ransom attacks involving multiple health care and billing systems, the bad actors may have gotten personal or financial information belonging to state employees. RSEA has had reports from members that hackers are sending texts, emails or calling, sometimes multiple times a day. All are phishing attempts to try and get your personal or financial information; the fraudsters are pressuring you to make immediate payments for a past due amount you really do not owe. The email, text, or call may even correctly identify certain details of a past health encounter such as: *this was from your appointment with Dr. Smith on July 1*. However real it may seem at the time; it is a **scam**.

Another recent phone scam reported to RSEA begins by saying there was a problem at your bank. Fraudsters may call you direct or your tablet/computer screen may flash a message indicating you need to contact your bank at the number shown (which is not your bank's.) Once a conversation begins, the fraudsters request you withdraw a hefty sum of money to save the money in your bank account - then they instruct you to convert it into bitcoin. The fraudsters even direct you to a particular bitcoin machine and stay on the phone with you while you complete the instructions. While you may say I would never do this, many times adrenaline and panic set in and common sense takes a back seat.

Whether email, text, phone, or mail, IF you have a doubt that the message is not legitimate, reach out and contact the individual or company though a method you have used previously. **Do not ask** GOOGLE, **do not ask** the internet, **do not reply** to their message. **JUST HANG UP**. Rely on your past conversations and use known contact information.

Preventatives to put into practice:

- Guard your personal identifying information.
- Lock down your credit information at all three credit reporting agencies. Place a fraud alert if necessary.
- Use good password practices on all online accounts.
- Refuse to engage with calls, emails, and text messages when you cannot confirm they are legitimate. Never click on any links or QR codes included in unconfirmed messages.
- Never feel pressured or rushed into sending money, purchasing gift cards, buying products, making donations, paying a bill, or signing contracts. Take your time.
- Use your caller-id and voice mail if you do not recognize a number.

If you think you have been a victim of a fraud report it:

- **Contact** your local police fraud unit.
- **Contact Illinois Office of the Attorney General Senior Citizens Consumer Fraud Helpline.** Call 1-800-243-5377 or email **seniorhelpline@ilag.gov.**
- Contact the **Criminal Division/Fraud Division of the Department of Justice Consumer Fraud and Identity Theft** at 1-877-FTC-HELP, 1-877-ID-THEFT, or online at https://ReportFraud.ftc.gov/#/?orgcode=TFMICF.
- **Health Care Fraud, Medicare/Medicaid Fraud, and Related Matters** Contact the Department of Health and Human Services, Office of the Inspector General at 1-800-HHS-TIPS, or online at www.oig.hhs.gov

WHEN IN DOUBT CHECK IT OUT.

Stay safe.
RSEA