



05-02-22

Recent Scams

Tip of the Day: Change the passwords on important accounts (credit card, banks, frequently used retailers, email etc) every three months. Make them “passphrases” – a random combination of words, plus numbers and symbols, to make them impossible to guess.

Every day our residents are contacted by scammers. These scammers will try to contact you via email, text, phone or sometimes by letter. They use various ploys in an effort to steal your money. Here are a few of the latest scams.

Text allegedly from the Apple Store. The text stated that the resident had made a \$560.00 purchase and to call an 800 number if there was any question about this purchase. This resident was very smart and alert and did not call the number. Had the resident called the number the scammer would have asked for personal information to verify that the resident was not the person owing the money. The scammer would try to obtain enough personal information which would allow him/her to have access to the resident’s bank or credit account. **Red flag** is notice of a large purchase you did not make.

Email “Confirming your order.” In this scheme the scammer (using a gmail address) informs in great detail that \$499 has been debited for McAfee antivirus software. “A full refund can be requested within seven days of your order. If you have any issues regarding your purchase, get help by calling +1 805 6195-657.” Again, the scammer would be seeking personal information. **Red flags** here are the nonstandard way the phone number is listed and the gmail address of the sender. There are other versions of this scam with different products, usually \$300 or more.

Help! I need Amazon Gift Cards. In this case the resident received an email that appeared to be from her pastor asking for a favor. The resident was told to purchase \$300.00 in Amazon cards and to keep it discreet. The email also said that this was urgent. The resident was to send the card numbers back to the person who had sent the email. This resident went to Safeway and when purchasing the cards was advised this may be a scam.

However, the resident did not believe the clerk and the card numbers were sent to the scammer. This resident later contacted the pastor and learned that this was a scam. She was not able to recover her \$300. This pastor was not named and is not involved; however he is from a nearby church and serves many seniors from SCLH.

These scammers can be very clever. Always be cautious of any message, phone call, text or letter from some person or company you do not recognize. When in doubt contact a relative, friend or neighbor for advice before responding to these unsolicited contacts. Also, be wary any time you are contacted by any person or organization that asks to be **paid with gift cards. Any mention of gift cards are a red flag.**

The recipient should change their password and notify the sender to change their password.

The April 2022 AARP Bulletin has an extensive article about scams, how they are perpetrated and a checklist for prevention. Only excerpts are available online. This one lists eight current scams <https://www.aarp.org/money/scams-fraud/info-2022/top-scams.html>

