SCAMS REPORT
S.A.L.T. COUNCIL MEETING OCTOBER 10, 2017
Submitted by Arnold H. Shifrin

"SMISHING"

Smishing is the fraudulent practice of sending text messages to cellular telephones in order to entice victims into sharing personal information. The term "smishing" is derived from combining ***SMS*** (Short Message Service, the technology used for cellular phone text messages) and ***"Phishing"*** (the use of Emails to obtain victims' personal information).

How it works: Scammers send thousands of text messages to potential victims with the hope that some will be gullible enough to take the bait. The messages state that "suspicious activities" have been occurring with the recipients' bank accounts or that the individuals are winners of a valuable prize. The unsuspecting victims are instructed to click on a link in the message or to call a number to resolve the bank account matters or claim their prize. Those who click on the link will be downloading viruses or other malware which allows the criminal to take control of the victim's phone. The criminal then has access to the victim's personal information such as bank account numbers, credit card numbers, user names, and passwords.

"Smishing" is becoming increasingly more prevalent because people tend to trust text messages more than Email messages and are not as likely to protect the personal information that's stored on their mobile phones. As a result, victims often follow the instructions from the criminals and wind up incurring large financial losses.

Steps you can take to avoid being a victim

- Be as vigilant about security for your mobile phone as you are for your desktop or laptop computer.
- Your mobile phone is essentially a pocket-sized computer that stores personal information, important documents, and other files. If a virus infects your phone, it can allow criminals access to your personal information.
- If you receive an unsolicited text message, do not respond and do not click on any links. Immediately delete the message.
- If you respond to the message, you are informing the scammer that your number is valid and that you will reply to messages sent to you. This puts you at risk for being targeted by other scammers.
- Check to see if your phone's app store offers anti-virus software. Some software may be available at no charge.
- Download apps only from trustworthy sources such as your phone's app store. If you download apps from third-party websites, you are placing your phone at risk.
- Keep your phone locked with a PIN or password when it's not in use.

(courtesy of AARP)