

By LARRY PHILLIPS • Leader & Times As communication technology advances, so does criminal fraud. Authorities are alerting the public concerning several new scams crossing the state, including two that have been reported in Liberal.

Seward County Sheriff's Detective Ryan McVey said one of the new scams involves texting and e-mails.

"People are getting messages – they can be through text messages or e-mails – that their credit card has been suspended," he said. "It's supposedly from a credit union and it looks very professional."

The message asks for verification of the credit card number, its expiration date and the three-numeral security number on the back.

It also had a message that says, "To reinstate your card, go to: (site withheld). That creates another problem.

"That link actually goes to a porn site, and as soon as it opens, it downloads a severe virus to your device," McVey said. "And it's over."

Another scam that has hit Liberal comes from a company that says it will settle your IRS problems. A Wichita tax attorney said such letters have been received by two of his Liberal clients. "The letters look very real – like they just might be from the IRS," the attorney said. "They, the scammers, are trying to get people who have tax issues with the IRS to settle for 10 percent of what they allegedly owe." In the letter, it says, "This letter is to notify (so-and-so) of a wage garnishment and tax lien investigation that may follow as a result of a tax lien that has been issued by the State of Kansas."

It goes on to say the victim has had a tax lien filed on a certain date in Seward County, and threatens that the "lien has been placed in the favor of the United States."

There are two hooks in the scam. The first being it says to contact the tax lien unit at (an 800 number) so you can immediately take care of the tax lien problem. The second hook is they'll let you off for 10 percent of what you allegedly owe, if you call and pay over the phone.

It specifically notes: "Do NOT send form of payment. Call us immediately."

Ironically, the second sentence below that order is a statement in small print that reads: "We are not associated with nor part of the Internal Revenue Service or any state agency."

"People who are having issues with the IRS are already upset, and this letter scares them into thinking they can get out of it for 10 percent," the attorney said. "But that money doesn't go to the IRS at all."

Local authorities are aware of that scam, and McVey had some advice for anyone that receives such a letter.

"First thing, any tax warrant for anyone in Seward County is served by the Seward County Sheriff's office," McVey said. "If anyone gets messages from the IRS – or what they think is the IRS – they should go to the IRS web site, get their phone number, and call 'that' number and start asking questions. They will let you know what's really going on."

The Better Business Bureau of Kansas is also warning area residents to be on the watch for phony tech support offers.

A consumer from Lecompton reported to the BBB that she had become a victim of a fake tech support phone call. She was recently contacted by a man with an accent who claimed that he was an engineer from her Internet service provider and needed access to her computer to fix error messages and viruses that he had detected.

Since the consumer had seen error messages, she typed a URL address which allowed the caller remote access to her computer. He proceeded to show her what was wrong on the monitor. Then he offered a two-year package that would fix all of her problems for \$199.

The consumer agreed to pay for this service and completed an online application giving her name, address, date of birth, Social Security number and her bank card information. As part of the application, she also gave permission to take money out of her bank account.

Two days later, she was contacted by another man who also had an accent. He informed her that the package she had purchased was not compatible with her computer, and in order to get the money refunded to her account, she needed to wire \$248 through Western Union to Uday Shanker in Gumta, India.

After the wire transfer had been completed, she received another call asking for the 10-digit number on the receipt and was promised that her money would be returned.

It has not, and she lost almost \$500.

McVey said the usual cautions should be used, don't give out any personal information to strangers, especially online.

"If someone is telling you there are problems – or if you think you're getting 'errors' – take your computer to an expert or certified repair place," he said. "Just unplug it and take it to him. That

way you're dealing with someone face-to-face, and you know who you're dealing with."

He also applies that to other suspicious letters or e-mails.

"If it's about finances, call your bank," he said. "If it's about the mortgage, call the mortgage company. If it's about the IRS, call them.

"If you think it's suspicious, contact local law enforcement and have it checked out," he added.

With the ever-increasing technology, McVey said it's creating more and more sophisticated thieves.

"It's the tech age," he said. "These people are thinking, 'why go door-to-door and rob people when we can do it on a computer,' and it's harder to find them."