AVOID THE SCAMS!

Q1 2017
by Security Chief Tim Moy

Most criminals are opportunistic in nature and will prey upon those who offer the greatest return at the lowest risk of being identified or prosecuted. Unfortunately, in many cases, seniors fall within this group and potentially make ideal targets. Staying informed and vigilant are the first steps to identifying and preventing a potential scam.

Jury duty scam: A call from a "representative" of the court alleges a failure to report for jury duty and an arrest warrant has been issued. The intended victim is offered a choice to either pay for the warrant or risk being arrested. The fraudster will typically demand money be paid by money transfer, wire or prepaid card.

IRS scam: This scam takes advantage of most Americans' inherent fear of the Internal Revenue Service. The phone call claims to be from the police or an IRS agent who is demanding payment for overdue taxes. The caller claims that if the overdue taxes are not wired immediately or put on a prepaid card, the victim will be arrested.

Lottery scam: This aims to convince targets they have won money in a lottery. The caller will advise that before collecting the winnings, the taxes, usually amounting to several thousand dollars, must be paid upfront.

Scareware scams: The scammer sends a pop-up "virus alert" claiming the target's computer has been infected. The target is then directed to download an anti-virus program resulting in identity theft or bank account access (at a fee) to remove the virus. The scammer is hoping a fake software program will be purchased and personal and financial information will be provided.

Grandparent scam: The intended victim will receive a phone call from someone posing as a grandchild who is supposedly out of town and in a desperate situation. The scammer then asks for money to be wired immediately.

Common themes include the grandchild is in jail, injured from a car accident, or stranded in a foreign country and in need of medical treatment.

On-line Romance Scam: Using email, scammers take advantage of lonely seniors, building false relationships and eventually professing their love. Some will even host fake Webcam sessions or call the victim on the phone. Once they sense the senior is falling in love with their false persona, the scam kicks into high gear. An "emergency" suddenly arises and the scammer pleads for money. The scammer can also want to meet the target but needs money to apply for a Visa.

Security Chief Tim Moy

To contact the Chief email him at
chief@vmsinc.org

Tips to Avoid Scams

Check Scam: Check scams involve a con artist offering to buy an item from a seller (often through Craigslist) using a cashier's check, which is made out for an amount that is greater than necessary. The scammer then asks that the check be cashed, and the excess funds returned. Of course, the check is fraudulent, but if the money is returned before the seller realizes this, they have lost the funds – as well as the item put up for sale.

Email/phishing scam: The intended victim receives email messages that appear to be from a legitimate company or institution, asking to "update" or "verify" personal information. Similar scams involve receiving a tax refund from the IRS asking to verify personal information.

If you believe you have been the victim of a scam or identity theft, please contact the Security Division at 949-580-1400. As it pertains to scams, you do not actually become a victim until you provide personal information or sustain a monetary loss. We will assess the situation and if necessary, contact the Sheriff's Department to open a criminal investigation.

Stay informed! Recognize that receiving an email, phone call or text message advising you won the lottery, failed to pay taxes, or need to update your account information is just another effort to gain access to your finances and personal information.

Sign up for email/text "transaction alerts" from your bank to keep track of your purchases.

Shred all financial documents, bank statements, sensitive mail, credit card solicitations, and documents that contain any type of personal information.

Report missing credit cards immediately. Use strong passwords for all services and change them regularly. When selecting a password, use at least eight characters, with a mixture of upper and lower case and both letters and numbers.

Be aware of your surroundings! Watch out for anyone attempting to watch you enter your PIN.

Keep current with anti-virus and anti-spyware software on your computer.

Use a credit card for online and mail order purchases. A credit card gives you better fraud protection than a debit card.

Sign up for the Federal Trade Commission free scam alerts at ftc.gov/scams for the latest tips and advice about scams.

Check the FBI website for additional scams at
www.fbi.gov/scams-and-safety/common-fraud-schemes