Frauds and Scams Alert

The Steger Police Department regularly receives reports concerning frauds and scams, including some instances of people impersonating Utility or even Village employees. In an effort to keep our residents informed, and thus reduce the number of victims, the Steger Police Department is alerting residents to the following:

Utility Disconnection Scam

In this scam, someone claiming to be with a utility company or village department calls utility customers and demands payment for alleged delinquent utility bill. The individual threatens to disconnect service if money isn't provided immediately. Technology event exists to allow fraudsters to make Village of Steger appear on your caller ID.
Remember: The Village of Steger Water Department will never request payment for delinquent utilities over the phone. You will receive a notice in the mail if your payment is overdue. If there is any question about the status of your Steger water account, contact the Village Hall at (708)754-3395.

"Can You Hear Me?" Scam

In this scam, someone will immediately ask "Can you hear me?" when you pick up the phone with the intent of getting you to say "yes". The caller may fumble around or say something like "I'm having trouble with my headset" to try to get you to respond. The Better Business Bureau warns that answering "yes" can be used by scammers to make it sound like you authorized major purchases like vacation packages, cruises, warranties and "other big ticket items."
Remember: If someone calls from a number you don't recognize and asks "Can you hear me?" do NOT answer "yes." Just hang up. In addition, scammers change their tactics as the public catches on, so be alert for other questions designed to solicit a simple "yes" answer.

Kidnapping Scam

In this scam, a scammer will falsely claim to be holding a loved one captive and demand an immediate ransom payment. Often, the caller will have some personal information about you or your family, making the call seem legitimate. The scammer will instruct you not to call the authorities, but to send a ransom by purchasing gift cards or wiring money.
Remember: Your best defense in such a scenario is to ask questions. Engage the caller in dialogue. Force the scammer to provide you more details, which the scammer doesn't have.

Arrest Scam

In this scam, the caller informs you that your loved one has been arrested and requests bond money for their release from jail. A similar scam involves a caller claiming to be a relative or friend, who asks you to send payment to get them out of jail.
Remember: If someone calls informing you that a loved one needs to be bonded out of jail, find out which jurisdiction the individual is in and call that agency directly to confirm that the person has, in fact, been arrested. Ask questions.

IRS Telephone Scam

Potential victims are told they are entitled to big refunds, or that they owe money that must be paid immediately to the IRS. When unsuccessful the first time, phone scammers often call back trying a new strategy. Immigrants are frequently targeted in this scam and are threatened with deportation, arrest, utility shut-off or having their driver's licenses revoked. Callers may insult victims in an effort to scare them.
Remember: The IRS will always send taxpayers a written notification of any tax due via the U.S. mail. The IRS never asks for credit card, debit card or prepaid card information over the telephone. For more information or to report a scam, visit www.irs.gov and type "scam" in the search box.

Tech Support Scam

Typically operating out of India, scammers call victims and allege that they're with a high-profile tech company. Victims are told their computers are either already infected or about to become infected with malware that can cause significant damage, such as operating system corruption or identity theft. The “technicians” then urge users to allow them to have remote access to troubleshoot and fix these issues. All of these actions permit scammers access to computers so they can cause errors, infect systems with malware or perform other damage and then charge for unnecessary repair services. It may also allow them access to personal and financial information.
Remember: Never give anyone remote access to your computer. Instead, hire a local computer repair service whenever necessary.

Grandparent Scam

In the Grandparent Scam, scammers call an older adult and say something similar to: “Hi Grandma, it’s me!” The grandparent then usually responds with the name of their grandchild, unwittingly giving the scammer identity information. The scammer then continues the conversation using the name the grandparent provided. They will usually ask for money to solve some unexpected financial problem such as a car accident, arrest or stolen wallet. Often times they may disclose that they are out of the country and thus need the money to be paid via Western Union or MoneyGram. The scammer will also ask the grandparent to keep this situation between them, as Mom/Dad would be mad if they knew they called. This prevents the grandparent from verifying the story given by the scammer. Sometimes the call may come not from the supposed grandchild, but from the scammer pretending to be a police officer giving the scam the illusion of credibility. And sometimes it’s not a phone call at all, but rather an email.
Remember: Resist the temptation to act quickly. Contact your grandchild or other family members to verify the information given in the call/email. Don’t wire money based solely on the information given over the phone or email.

Fraudulent/Fake Check Scam

With this scam, victims are tricked into accepting fraudulent or fake checks. This is very common when the victim is selling something through the internet or an ad in the newspaper. Victims will receive a check for a much higher amount than agreed upon. The scammer may give a variety of reasons as to why this has occurred. They eventually convince the victim to send back the overpayment via non-returnable methods, such as wire transfers. Eventually, the scammer’s check bounces and the victim realizes that they have been conned.
Remember: Never accept checks with amounts over the agreed upon price and never send money back. If you are selling an item on the internet or elsewhere, make sure that the check has cleared the bank before releasing the merchandise to the buyer.

Phishing

Scammers pretend to be legitimate organizations/companies and send an official looking email or contact victims via phone, to get them to reveal sensitive data. If you get an email or pop-up asking for personal or financial information, don’t reply. Do not click on any pop-ups. Do not give out personal information over the phone unless you have initiated the phone call and know to whom you are speaking.
Remember: Legitimate companies will not ask for sensitive information over the phone or via email. Never give anyone you don’t know information concerning bank accounts, passwords, social security numbers, etc. Contact the organization/company using a phone number you know as genuine. Also, keep your computer's anti-virus and anti-spyware software up-to-date.

Foreign Lotteries or Sweepstakes

The victim is informed via email, phone or postal letter that they have won a lottery but that in order to claim their prize money, the victim will have to send a check for fees, taxes or insurance. The scammers may send a check for the lottery winnings, and although the check shows up in the victim’s bank account, soon after the "fees" are collected from the victim, it is discovered that the check is fraudulent. In a variation of this scam, a check comes in the mail to cover “taxes, fees or

insurance” and the recipient is asked to cash the check and wire back funds to claim the prize. However, the original check is no good.
Remember: It is illegal for U.S. citizens to enter foreign sweepstakes or lotteries. Also, if you have to send money, even if they send you a check, it is a red flag.

Collection Agency Scam

In this scam the perpetrators tell victims that they are representatives from a collection agency. They make cold calls to victims and threaten lawsuits or embarrassing on-the-job confrontations unless the victims start making payments. Fee payment is to be made by non-returnable methods, such as MoneyGram, Western Union or wire transfer. Scammers may even have actual information about a real outstanding loan. Harassment may go on for months.
Remember: Do your homework and make sure that if you have a bad debt and owe money to a collection agency, you know who you are dealing with. Block all other collection calls.

Fake Arrest Warrant Scam

Victims receive phone calls, emails and/or faxes stating that arrest warrants have been issued in their name. They are then instructed to call a number to make arrangements in order to avoid arrest. “Fake” law enforcement officials request a settlement be paid via wire transfer, money order or prepaid credit card. Warrants are made to look official and may even display a logo of an unspecified “United States District Court,” a case number and/or various charges. Many of the fake warrants are for offenses such as missed jury duty or bank fraud.
Remember: A valid arrest warrant is served in person by a U.S. Marshal or other law enforcement officer.

Obituary Column Scam

The scammer reads the obituary column and then presents fake bills to the surviving spouse explaining that these were owed by the deceased. Sometimes, the scammer may deliver packages that are presented as items the deceased ordered and now payment is due.
Remember: Verify all outstanding bills with the appropriate company/business. Do not accept any packages you did not order personally.

Bank Examiner Scam

In this scam the perpetrator poses as law enforcement or as a bank employee and ask for the victim’s help in catching a dishonest teller. They ask the victim to withdraw a certain amount of cash from their account and to then give it to them in order for the serial numbers to be checked. Once in the hands of the scammers, the money and the scammer are nowhere to be found.
Remember: Banks do not ask customers for assistance in flushing out dishonest employees.

Utility Scam

In this scam, someone claiming to be with a utility company comes around during an outage and offers to reconnect the victim's service for a cash payment. The victim thinks it’s a bit odd that the person is asking for cash, but rationalizes the visit by thinking the company’s power is out, too, and they can’t operate the computers to process payments. The visitor looks and sounds legitimate, and the victim really needs their service turned on. The victim pays, and hours later there are still no utilities and no sign of the person. Eventually, the utility company restores the service, not the so-called “representative” who took the money.
Remember: Local utilities, including the Village of Steger, will never send someone around door-to-door during an outage asking for money to restore services.
Report
Please do not hesitate to contact the Steger Police Department with any questions or concerns, especially if you think you may have been victimized. Better to be safe than sorry.