Cheshire Police

Community Service Bulletin

The Cheshire Police Department would like to make the public aware of several common scams that have victimized and defrauded Cheshire residents in the past three months. In total, three residents have collectively lost $169,000 to predators targeting them using scams. In the three recent cases, the victims were aged 67, 79, and 81. The criminals responsible for these scams are known to target senior citizens.

In September, a resident was targeted using the “grandparent” scam. The victim received a phone call from a person claiming to be her grandson saying that he was involved in a car accident and had injured a pregnant woman. The “grandson” told the victim that his attorney would be calling her with further information. The perpetrator, posing as the grandson’s lawyer, told the victim that $25,000 was needed to bail her grandson out of jail. The victim was instructed to withdraw the money from her bank so it could be picked up by a “bail bondsman”. The victim complied with the instructions and provided $25,000 in cash to a person who came to her residence. Later that same day, the same perpetrator called the victim back, told her that her grandson had been rearrested for talking about his case after being released, and that an additional $20,000 cash was needed to secure his release. The victim complied with the second demand also. In both instances, the victim was questioned by a bank employee about the large cash withdrawals. The scammers told the victim that this may happen and instructed her to tell the bank that she was buying a car for her grandson. After the second cash payment had been picked up, the victim called her grandson and learned that he was fine and that she was the victim of a scam.

Scams like this are becoming increasingly sophisticated using artificial intelligence (AI). Some reporting indicates that AI is being used to mimic the voice of the loved one who is allegedly in trouble.

The two incidents that occurred in November are variations on the “technical support” scam where predators pretend to be technical support employees of known companies who can help with a computer problem. In one case, the victim used a common online search portal to contact technical support for her computer. The website she located was designed to look like a legitimate technical support provider for a well know technology company. In fact, it was a fake site run by scammers who stole $95,000 from the victim. The second case involved a victim who clicked on a “pop-up” message on her computer claiming that her anti-virus protection had expired. The link lead to scammers who ultimately stole $29,000 from the victim.

These scams are also becoming more sophisticated. The victims received official looking, but false, correspondence claiming to be from the Federal Trade Commission and the United States Treasury Department. The letters had names and official sounding titles and in one case the victim spoke on the phone multiple times with a person claiming to be a “fraud investigator”.

There are two major red flags that should make anyone suspicious. The first is providing usernames and passwords or other information that a third party can use to access your computer and accounts remotely. The second is any request or instruction that you withdraw cash or precious metals like gold or silver to make a payment or secure your funds.

Cheshire Police

Community Service Bulletin

As the criminal organizations behind these scams have become more sophisticated, so has the law enforcement and private sector response. Law enforcement has become more adept at recovering money that is being transferred through electronic means. That is why scammers often insist that cash or precious metals are the only way to complete the fraudulent transactions. Retail and financial sector employees have been trained to spot potential scams victimizing their customers, such as large cash withdrawals or large purchases of gift cards. That is why scammers provide victims with reasons to support their activity, such as one of the Cheshire victims telling the bank employee that she was buying a car for her grandson.

If you have any doubt about the validity of solicitation you receive, please do not hesitate to contact the Cheshire Police Department or a trusted family member to discuss the issue before engaging in any financial transaction.

The following bulletin was produced by the FBI that contains further information about common criminal scams.

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-012924-PSA
January 29, 2024

Scammers Use Couriers to Retrieve Cash and Precious Metals from Victims of Tech Support and Government Impersonation Scams

The FBI is warning the public about scammers instructing victims, many of whom are senior citizens, to liquidate their assets into cash and/or buy gold, silver, or other precious metals to protect their funds. Criminals then arrange for couriers to meet the victims in person to pick up the cash or precious metals. From May to December 2023, the FBI Internet Crime Complaint Center (IC3) saw an uptick in this activity with aggregated losses of over $55 million.

Step 1: Scammers Instruct Victims to Liquidate Assets into Cash and/or Buy Precious Metal

Scammers pose as tech support or US government officials. Scammers sometimes use a multi-layered approach, posing, in succession, as a technology company, a financial institution, and a US government official (e.g., the "Phantom Hacker" scam). Scammers inform victims their financial accounts were hacked or are at risk of being hacked, and, as a result, their funds need to be protected. Scammers instruct victims to liquidate their assets into cash and/or purchase gold, silver, or other precious metals. Sometimes, scammers instruct victims to wire funds to a metal dealer who will ship the precious metals to victims' homes.

Step 2: Scammers Use Couriers to Retrieve Cash and/or Precious Metals from Victim

Once victims obtain the cash and/or precious metals, the scammers send couriers to retrieve the items at victims' homes or public locations. Scammers may direct victims to authenticate the transaction with the courier using a passcode, such as the serial number of a US dollar bill. Scammers tell victims they will safeguard the assets in a protected account on behalf of the victims. In reality, victims never hear back from the scammers and lose all their money.

TIPS TO PROTECT YOURSELF

- The US Government and legitimate businesses will never request you purchase gold or other precious metals.

- Protect your personal information. Never disclose your home address or agree to meet with unknown individuals to deliver cash or precious metals.
- Do not click on unsolicited pop-ups on your computer, links sent via text messages, or email links and attachments.
- Do not contact unknown telephone numbers provided in pop-ups, texts, or emails.
- Do not download software at the request of unknown individuals who contact you.
- Do not allow unknown individuals access to your computer.

REPORT IT

The FBI requests victims report these fraudulent or suspicious activities to the FBI IC3 at www.ic3.gov as quickly as possible. Be sure to include as much transaction information as possible:

- The name of the person or company that contacted you.
- Methods of communication used, including websites, emails, and telephone numbers.
- Any bank account number(s) to which you wired funds and the recipient name(s).
- The name and location of the metal dealer company and the account to which you wired funds, if you were instructed to buy precious metals.

Victims aged 60 or over who need assistance with filing an IC3 complaint, can contact the DOJ Elder Justice Hotline, 1-833-FRAUD-11 (or 833-372-8311).

For additional information on similar scams or fraudulent activity, please see the previous Public Service Announcements:

- IC3 | "Phantom Hacker" Scams Target Senior Citizens and Result in Victims Losing their Life Savings
- IC3 | Technical and Customer Support Fraud
- IC3 | Increase in Tech Support Scams Targeting Older Adults and Directing Victims to Send Cash through Shipping Companies
- IC3 | Scammers Using Computer-Technical Support Impersonation Scams to Target Victims and Conduct Wire Transfers