Common Cryptocurrency Scams Targeting Seniors

Milton Township S.A.L.T. Council Meeting
April 14, 2025

Presented by: Arnold H. Shifrin, RPh
Director of Communications
Milton Township S.A.L.T. Council
Email: ahshifrin@gmail.com

Cryptocurrency - Background and Definitions

1. Fiat currencies: stable currencies issued and regulated by governments and central banks.
    - U.S. Dollar (USD)
    - Euro (EUR)
    - British Pound (GBP)
    - Japanese Yen (JPY)
    - Chinese Yuan (CNY)
2. Cryptocurrency: highly volatile decentralized digital currency that relies on blockchain technology and cryptography for security. There is no governing body controlling cryptocurrency values. There are thousands of active cryptocurrencies.

3. Top 5 Cryptocurrencies Ranked by Market Capitalization *

	Cryptocurrency	Symbol	Market Capitalization
1.	Bitcoin	BTC	$458 billion
2.	Ether	ETH	$216 Billion
3.	Tether	USDT	$66 billion
4.	USD Coin	USDC	$54 billion
5.	Binance Coin	BNB	$52 billion

* Market capitalization (aka "market cap") is the total dollar value of the cryptocurrency in circulation.

4. Blockchain: a digital ledger that records and stores cryptocurrency transactions and account balances.

5. Cryptocurrency exchanges: online platforms where you can buy, sell, and trade cryptocurrencies, similar to the way stock exchanges operate for stocks. There are currently more than 500 exchanges.
   a. Binance
   b. Coinbase Exchange
   c. Kraken
   d. KuCoin
   e. Binance.US
   f. Bitfinex
   g. Gemini
   h. Coincheck

6. Cryptocurrency wallet: a digital tool that allows you to manage your cryptocurrency holdings on a blockchain.

7. Bitcoin ATMs: small standalone digital devices (kiosks) that enable users to buy or sell Bitcoins, using cash or a credit/debit card to access their digital wallets. These ATMs are found in retail establishments (e.g., Costco, CVS, Walgreens, Walmart, and convenience stores).

8. According to the FBI, people aged 60+ reported losses of more than $1.6 billion to cryptocurrency scams in 2023.

9. Cryptocurrency is considered by the IRS as property, not currency, and is subject to capital gains taxes when sold or exchanged. Crypto exchanges are required to report transaction details to the IRS.

10. Cryptocurrency is not legal tender, and businesses are not required to accept it for payment of goods or services.

Romance Scams

- Characterized by a long, methodical process of online seduction, usually by someone the victim typically meets on a dating site.
- Victims are groomed over time for financial exploitation.
- Scammers share their knowledge of investing and claim they received large returns by investing in cryptocurrency; they eventually convince their victims to invest in cryptocurrency.
- Victims create an account, receive a digital wallet, and fund their accounts with cryptocurrency purchased with fiat currency.
- As fake profits are posted to their account, victims are encouraged to deposit larger amounts.
- When they try to withdraw funds, victims are told they owe outrageous amounts for taxes and fees and are shut out of their accounts.
- Scammers vanish with all the money.

Investment Scams

- Similar to romance scams, but without the emotional component.
- Also called "pig butchering" scams, as they are analogous to the fattening of pigs before slaughter.
- Scammers pose as phony investment managers to lure victims with promises of rapid growth and high returns on cryptocurrency investments.
- Fake, well-designed websites and phony celebrity endorsements are used to entice victims to invest.
- Scammers steal the invested funds, causing victims to lose all their money.

ICO (Initial Coin Offering) Scams

- ICOs are a way for companies to raise capital by selling new cryptocurrency to investors. ICOs are similar to IPOs (Initial Public Offerings) for stocks.
- Scammers convince victims to invest in ICOs on cryptocurrency exchanges to inflate the price of the currency.
- Once enough victims have invested, scammers quickly sell off their holdings, causing the value of the currency to crash and leaving investors with worthless assets.
- ICOs are unregulated, very risky investments, and are prone to scams and fraud.

Impostor Scams (aka Impersonation Scams)

- Scammers pretending to be from trusted sources such as government agencies, banks, credit card companies, or utility companies contact victims under the pretense of collecting delinquent taxes or past due balances.
- Victims are instructed to remit payment in cryptocurrency to settle the matter and are threatened with arrest and imprisonment if they fail to do so.
- Warning: Do not trust your caller ID. It can be manipulated to show a different caller than the one originating the call ("spoofing").

Tech Support Scams

- Scammers contact victims and pretend to be computer technicians from a well-known company (e.g., Geek Squad).
- Victims are told a "problem" (e.g., a virus or malware) was found with their computer, and they are urged to grant the technician remote access so diagnostic tests can be run and repairs made.
- After remote access is granted, victims are told the problem was found. They are instructed to transfer cryptocurrency to the scammer's account to pay for the bogus repairs.
- Warning: once a scammer has remote access to your computer, your PII (personally identifiable information) is significantly at risk.

Phishing / Smishing Scams

- Scammers send fraudulent emails ("phishing") or text messages ("smishing") that appear to originate from legitimate entities to trick victims into revealing personal information, including the login credentials to their cryptocurrency wallets.
- Once the scammers gain access to the wallets, they transfer the funds to their accounts.

How To Avoid Being A Cryptocurrency Scam Victim

- Do not send cryptocurrency to someone you don't know or have not met in person.
- Verify all requests for payment by cryptocurrency before remitting, using contact information for the payee that you know is correct.
- Be wary of requests for mandatory payments with cryptocurrency, as these are likely scams. Crypto payments are difficult to trace and cannot be reversed.
- Create a strong password for your cryptocurrency wallet and enable 2FA (two-factor authentication).
- Talk with a knowledgeable financial advisor before investing in cryptocurrency
- Read legitimate industry publications to learn the technology and terminology.
- Beware of high-risk investments; do not invest more money than you can afford to lose
- Before investing, make sure the company is registered with the CTFTC (Commodities Futures Trading Commission) and a member of the NFA (National Futures Association)
- Never grant anyone remote access to your computer unless you initiated the contact and trust the individual.
- Do not divulge your PII to anyone until you verify who is requesting it.

If you are a victim of a cryptocurrency scam, notify the following agencies:

- Illinois Attorney General's Senior Citizens Consumer Fraud Helpline:
  - Tel: 1-800-243-5377 or
  - Email: seniorhelpline@ilag.gov.
- FBI's Internet Crime Complaint Center: www.ic3.gov.
- Your local police department.

Thank you for your interest and attention. We hope you found this information helpful. Stay safe!

Questions and Comments?