Nicolet NATIONAL BANK

SCAM AWARENESS BULLETIN

Real People. Real Conversations.

Avoid Scams Involving Virtual Currency Kiosk or "Bitcoin ATMs"

Introduction

Fraudsters and con artists often convince unwitting consumers to send payments via gift cards and money transfers. Now, scammers are increasingly stealing money using cryptocurrencies such as Bitcoin, often telling consumers to use so-called virtual currency kiosks (also known as Bitcoin ATMs). These machines look and operate like bank ATMs, and they allow scammers to receive payment in cryptocurrencies such as Bitcoin, Ethereum, and Tether. Although tactics vary, criminals create a false sense of urgency and trick victims into withdrawing cash from their bank account. The scammer then directs the consumer to deposit the cash into a virtual currency kiosk. The consumer purchases the virtual currency which is then sent to the scammer's crypto wallet.

How it Works

Tactics include the following:

- "**Romance scams"** start when con artists contact victims through online social networking and dating apps, gain trust over time, and make promises. In the end, scammers tell lies and request money for false purposes including emergency medical or legal fees. After inducing victims to send payments via a virtual currency kiosk, the con artist disappears.

- "**Pig butchering" scams** often begin with the victim receiving a random text message from an unknown number. Scammers strike up conversation with victims, then move the discussion to a messaging platform such as WhatsApp. After establishing a phony relationship over weeks or months, scammers then pitch fail-safe cryptocurrency investments. Scammers then direct victims to "invest" cash using a virtual currency kiosk, with instructions to send cryptocurrency to an" investment site" – which is actually the scammer's own crypto wallet.

- **"Investment adviser**" scams involve inducing victims to make initial investments on bogus trading platforms, then gaining trust by showing investment gains. Victims transfer increasingly large sums only to learn they have been scammed when they are locked out of their accounts.

- Computer "anti-virus protection" scams occur when victims fall for bogus "pop-up" alerts on their computer screens. Victims follow directions to call a "help-desk" number to receive antivirus protection. Scammers posing as customer service staff convince victims that hackers have access to their bank account and that they need to convert their cash to cryptocurrency via a virtual currency kiosk. Of course, scammers end up with the cryptocurrency and then disappear.

- Scammers pose as **electric utility companies** and threaten to cut off power to the victim's home unless a payment is made via a virtual currency kiosk.

What to Do

It is important for consumers to keep in mind that only scammers demand advance payment in cryptocurrency, gift cards, or money transfers. No legitimate business will request advance payment in cryptocurrency, including through a virtual currency kiosk. Cryptocurrency payments made to scammers via virtual currency kiosks are typically not reversible. **Once sent, the money is gone!**

To avoid becoming a victim, do not pay anyone who contacts you and demands advance payment in cryptocurrency, gift cards, or money transfer. You can learn

more about the risks of paying with cryptocurrency here. If anyone asks that you withdraw cash from your bank account and convert it into cryptocurrency at a virtual currency kiosk you should take the following precautions

- Ask questions and don't provide personal information.
- Contact a relative, friend, neighbor, or other trusted person and ask for advice.
- If the person demanding payment tells you they are from your bank, utility company, or another business, contact the published customer service number of the business to confirm the identity of the person.

Work Cited:

Avoid Scams Involving Virtual Currency Kiosk or "Bitcoin ATMs" as found at Joint-Consumer-Alert---Virtual-Currency-Kiosk.pdf (ct.gov) on September 18, 2023.