Are You an Informed Investor?
Bitcoin ATMs

July 2025

Bitcoin ATMs are playing a bigger role in Bitcoin scams than ever before. Data from the Federal Trade Commission shows consumers reporting over $110 million in losses to scams involving Bitcoin ATM machines in 2023, a tenfold increase since 2020.[1] Fraudsters are capitalizing on the increasing popularity and accessibility of these machines, and they are employing tried-and-true high pressure tactics against their targets to entice them into using the machines to transfer money or other crypto assets to accounts the fraudsters control. It is important for consumers to understand what Bitcoin ATMs are, how the scams work, and what consumers can do to protect themselves.

---

1 Bitcoin ATMs: A payment portal for scammers. (2024, September 3). Emma Fletcher, Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2024/09/bitcoin-atms-payment-portal-scammers

What Are Bitcoin ATMs?

A Bitcoin ATM (also known by a number of other names, including Crypto ATM) is an electronic kiosk designed to facilitate buying cryptocurrencies using any financial transaction card, including a credit card or debit card. These machines look like traditional ATMs and are located in all the same kinds of places: gas stations, convenience stores, malls, and other high-traffic areas. How can spoofing and phishing affect investors?

How Do Bitcoin ATMs Work?

You can deposit money into the ATM and the ATM charges a fee and transfers the money into cryptocurrency and puts it into an electronic wallet. You provide the address of the wallet.

Using Crypto ATMs to Facilitate Scams

While these machines provide convenient access to digital currencies, legitimate Bitcoin ATMs are increasingly being used as key players in crypto or Bitcoin scams.

The scams start through chats, social media, emails, texts, pop ups, and phone calls from strangers. The lies told by scammers vary, but they create some urgent justification for consumers to take cash out of their bank accounts and put it into a Bitcoin ATM. Often, the scammers fabricate an investment that promises great returns with limited risk. When consumers put money into a Bitcoin ATM, the ATM converts the money to cryptocurrency. The consumer types in the scammer's electronic wallet address, or the consumer is given a QR code to scan which points to the scammer's electronic wallet address. The Bitcoin ATM then transfers the crypto to the scammer's electronic wallet. Once in their control the scammers quickly move the crypto making it very difficult to trace and recover.

How to Protect Yourself

- Slow down. Scammers want you to rush out to the nearest Bitcoin ATM, put in your money, and send crypto to them. Pause, take a minute first. If you have been directed by someone to make a payment using a Bitcoin ATM, it is very likely that this is a scam.

Continued

- Never click on links or answer unexpected calls, messages, or computer pop-ups. Don't respond to the person who contacted you. Delete the message and report it as junk to your carrier.

- Never withdraw cash in response to an unexpected call or message. Only scammers will tell you to do that.

- Don't believe anyone who says you need to use a Bitcoin ATM to protect your money, or to fix a problem, or to get in on a great investment. Real businesses and government agencies will never do that – and anyone who asks is a scammer.

- Because ownership of virtual wallets and addresses is anonymous, a crypto ATM operator cannot feasibly prevent its machines from being used for money transmission. However, some states are amending their money transmission laws to make them applicable to crypto ATM operators. Consumers may wish to contact their state's banking regulator for more information about what protections exist in their jurisdiction.

Be cautious if someone tells you something is a secret or information cannot be shared with anyone. Compelled silence is a method used by scammers which isolates individuals from trusted resources. Remember, most Bitcoin ATMs:

- Do not limit how much money you can deposit into the machine, so there are no limits on how much you can lose;

- Do not verify the identities of either the sender or recipient of a crypto transaction, thereby making recovery or tracing very difficult;

- Do not register with any U.S. governmental agency, so state government agencies have a difficult time providing help;

- Do not have any fraud prevention or reimbursement policy; and,

- Do not limit transaction fees which can be very high.

The Bottom Line

The important thing to remember about crypto transactions, is that they are designed to be anonymous and instantaneous. Most investment losses due to cryptocurrency investments are unrecoverable and your money is gone forever. For more tips and information about how to be a better informed investor, contact your state or provincial securities regulator. In Connecticut, contact the Department of Banking, at CT.gov/dob.

Connecticut Department of Banking
Securities and Business Investments Division
CT.gov/dob | 1-800-831-7225

CONNECTICUT
Department of Banking