CRYPTO ATMS

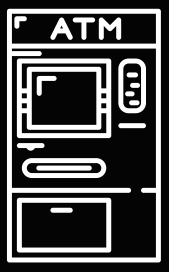
Crypto automated teller machines (ATMs) are stand-alone electronic kiosks that allow users to buy and sell cryptocurrency in exchange for cash or with a debit card.

Coinme is the Official exchange for Bitcoin ATMS. There are more than 10,000 Bitcoin ATMs around the U.S. The Coinme software allows users to deposit cash in a Coinstar ATM and exchange it for a Bitcoin voucher. The voucher has a specialized code and PIN that can be used with the Coinme mobile app to redeem the deposits for Bitcoin.

The Coinme App is a cryptocurrency exchange and digital wallet that is used to buy and sell cryptocurrency, and to store bitcoin and other supported cryptocurrencies on the Coinme platform.

ATM RISKS

There are risks with using Crypto ATMs.



A con artist may convince a victim to put cash into a cryptocurrency ATM and send the purchased coins to the scammer using an address stored in a QR code via CoinDesk.

There have been $3.2 billion stolen through crypto hacks in 2021 alone.

There are also High Fees when using Coinme. Coinme charges a 4% transaction fee for buying or selling and also charge a transaction fee.

There is no insurance available. Coinme does not offer insurance, so user funds are not protected. Funds stolen or lost will not be reimbursed.

Recognizing red flags like guaranteed returns, lack of transparency, and pressure to act quickly can help identify cryptocurrency scams.

SCAMS

Phishing Scams: Scammers often create elaborate clones of profiles, websites, emails of a company they are impersonating. Victims are phished after being contacted by a seemingly reputable company.

Phishing scams promise unrealistic returns on a new offer, promotion, product, or service.
Thye also may contain links that require victims to enter their private keys or recovery phrases or will offer to resolve a technical issue.

Avoid clicking any links or ever giving private keys. Never enter your credentials anywhere other than the official apps or websites.

Romance Scams: A scammer manipulates a victim into giving them money after professions of love.

Avoid this scam by thinking rationally rather than emotionally if you meet someone who is asking for money.

Pig Butchering Scams: Similar to Romance scams, con artists begin a relationship and earn trust. Once they have trust they will encourage the victim to invest in cryptocurrencies in an effort to help make the victim rich. The con artist will "help" the victim find a platform for them to invest in and then extract the funds.

Withdrawal Scams: in these scams the scammer will allege that they are unable to withdraw funds and request assistance of the victim in return for a share of the funds.

Scammers may request help with withdrawal of actual funds in a wallet controlled by the scammer, who will claim they are having difficulties withdrawing. The victim will then send crypto to a wallet hoping to extract funds from it. Scammers will have a bot that monitors the wallet and will withdraw any funds transferred to it.

To avoid theses scams, avoid under the table dealings, no matter how great they sound. If someone offers you their seed phrase - it is likely too good to be true.

Cryptojacking: This cybercrime is done when a hacker co-opts a victims' computing power to secretly mine cryptocurrency on the hacker's behalf. Cryptojacking is easy, cheap and profitable for scammers.

To avoid Cryptojacking only install software from trusted sources, don't fall for phishing emails and consider using ad blockers in your browser or disable JavaScript.