

HOW THE BITCOIN ATM SCAM WORKS



1.

Scammers Initiate Contact

Scammers may reach out via phone, email, or text using information they've obtained from publicly available social media profiles, data leaks, or even the dark web.



2.

Scammers Pose as Authorities

Scammers often impersonate individuals or organizations you trust.

- Government officials (e.g., FTC, FBI, IRS, U.S. Treasury)
- Tech support from well-known companies (e.g., Microsoft, Apple)
- Bank representatives
- Law enforcement officers



3.

Scammers Create a Sense of Urgency

Scammers will claim you are in trouble, using scare tactics to push you into quick action.

They may allege:

- Suspicious activity in your bank account
- Unauthorized access to your devices (e.g., computer, phone)
- Your personal information being used in crimes
- Your money is at risk of being stolen
- A loved one has been involved in an accident or emergency



4.

Scammers Direct You to a Bitcoin ATM

Scammers will direct you to deposit cash into a Bitcoin ATM, providing a QR code linked to their wallet.

Once completed, the transaction is irreversible and nearly impossible to trace.



How To Avoid This Scam

Seek advice from a trusted friend or family member, no matter how urgent the caller sounds.

Legitimate representatives or government officials will never discourage you from consulting others, request cryptocurrency payments, or demand immediate action.