

How to spot a Bitcoin ATM cash deposit scam

[Read online: https://cyberguardlab.com/blog/bitcoin-atm-cash-deposit-scam](https://cyberguardlab.com/blog/bitcoin-atm-cash-deposit-scam)

Published October 13, 2026 | Updated October 13, 2026

Short answer

A Bitcoin ATM cash deposit scam is an unexpected call or message that tells you to withdraw cash from your bank, investment, or retirement account and feed that cash into a Bitcoin ATM (also called a BTM or cryptocurrency kiosk) - usually after the caller texts a QR code for you to scan - supposedly to "protect" your money, fix a fake account problem, or pay a fake government or bail demand. The Federal Trade Commission's September 3, 2024 consumer alert explains that once the cash goes into the machine under the scammer's QR code, it goes straight into the scammer's wallet. The FTC's March 7, 2024 alert says nobody legitimate sends you to a Bitcoin ATM, government never does, and there is no government Bitcoin account or federal "safety locker." This page is about the physical cash-into-kiosk payment step: withdraw cash -> specific machine -> QR to scammer wallet, often with the caller coaching you to stay on the phone. Broader fake crypto investment platforms are covered in this site's cryptocurrency scam guide. Guides on CyberGuardLab are written as independent consumer explainers. Some product pages elsewhere may include affiliate links that affect which tools are listed. The checklist on this page costs nothing; any paid antivirus or identity product appears only in the closing section if you want it.

Advertising disclosure: CyberGuardLab is an independent comparison site. We are not TotalAV, Norton, Bitdefender, McAfee, or Avast. If you buy through our links, we may earn a commission, which can affect ranking and placement.

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.

CYBERGUARDLAB · GUIDE

How to spot a Bitcoin ATM cash deposit scam

Hang up before you feed cash into a kiosk someone just named.



What to do in the first minute

End the call. Leave cash in the account. Skip every Bitcoin ATM, crypto kiosk, or cash-to-crypto machine that an unexpected voice or text just named. No real bank, retailer, or government desk sends people to a BTM to "protect" funds or clear a fake problem. If an Amazon, bank, brokerage, or agency issue might be real, open that brand's official app or dial the line you already saved - never the number inside the surprise message. If cash already went into a machine, use the customer line on your bank statement or the official banking app, keep the receipt and any QR screenshot, then open [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud) and a separate [IC3.gov](https://www.ic3.gov) complaint.

How a Bitcoin ATM cash deposit scam works

Official FTC and FBI pages describe a cash-to-kiosk path that is easy to miss until the bills are gone:

Paid link

Norton 360 | See the Norton first-year offer



[See the Norton first-year offer](https://cyberguardlab.com/norton)

Offer page: <https://cyberguardlab.com/norton> Hop: <https://trysecurities.com/offer/norton?dtm=gg&cid=>

* The opener invents a problem you feel you must fix. The FTC's September 2024 alert says many of these scams start with a call or message about something supposedly wrong - for example suspicious activity on an Amazon account or unauthorized charges on a bank account. The story may escalate to claims that your money is at risk or that you are linked to money laundering or drug smuggling. The FBI's September 17, 2026 IC3 PSA (an update on law-enforcement and government impersonation) adds that callers often accuse you of a crime, missed jury duty, or a warrant and demand payment to avoid arrest.

* They keep you on the phone and alone. The same FBI PSA says scammers use urgent, aggressive tones, refuse to speak with anyone but the targeted victim, keep victims on the phone for the duration of the scam, and urge them not to tell family, friends, financial institutions, or law enforcement. A second trusted person would often stop the deposit.

* The "solution" is to move cash into a machine. The FTC's September 2024 alert says the caller tells you to withdraw cash from your bank, investment, or retirement accounts and deposit it into a specific Bitcoin ATM to protect your money or fix the alleged problem. The FTC Data Spotlight dated September 3, 2024 notes that scammers have even called these machines "safety lockers." The March 2024 FTC alert states there is no such thing as a government Bitcoin account or digital wallet and no Bitcoin federal safety lockers.

* They send you to a specific kiosk with a QR code. The September 2024 Data Spotlight explains that scammers direct you to a nearby BTM location - often a specific one - then text a QR code to scan at the machine. Once you scan and deposit, the cash goes into the scammer's wallet. The September 2024 FTC press release repeats the same QR-to-scammer-wallet step.

* Payment methods are chosen so reverse is hard. The FBI PSA lists cash inserted into cryptocurrency kiosks alongside prepaid cards, couriers, bank wires, and cryptocurrency as demanded payment methods. Cash into a kiosk under someone else's QR code is not a reversible bank transfer.

* Impersonation stories vary; the kiosk step stays the same. The Data Spotlight says reports of losses using BTMs are overwhelmingly about government impersonation, business impersonation, and tech support scams. A pop-up that funnels you onto a phone line may start as a tech support scam phone call; Social Security, jury-duty, or tax stories may sound like those separate guides. This page focuses on the moment someone tells you to put cash into a BTM.

Cash-to-kiosk red flags

Red flag | Why FTC or FBI call it out | Your move

Caller says a Bitcoin ATM or "safety locker" will protect your money | FTC March 2024: no government Bitcoin account; no federal safety lockers. Spotlight: scammers have called BTMs "safety lockers." | Hang up; your money stays safer in the real account

You must withdraw cash from bank, investment, or retirement accounts | FTC September 2024 alert describes this exact step before the BTM deposit | Do not withdraw; call the institution on its published customer line

A QR code arrives by text for you to scan at a specific machine | Spotlight and FTC press release: cash under that QR goes to the scammer's wallet | Do not scan; save the text for your report

Stay on the phone and tell no one | FBI PSA: keep victims on the phone; urge secrecy from family and banks | End the call; tell a trusted person and your bank

Story mixes Amazon/bank "fraud," tech support, or government arrest threats with a kiosk payment | Spotlight: BTM loss reports are overwhelmingly government, business, and tech-support impersonation | Treat the payment channel as the stop sign regardless of the story brand

BTM coaching call vs legitimate bank contact

Cue | Coached kiosk deposit | Bank or agency you dial yourself | After you reach a published number

How contact starts | Unexpected call, text, email, or pop-up number you did not look up yourself | You initiate contact from a statement, official app, or known public number | The real fraud desk or agency has no open "deposit cash in a Bitcoin ATM" case for you

What they ask | Withdraw cash and feed a named BTM / crypto kiosk, often with a QR texted to your phone | Never asks you to move money into a Bitcoin ATM to "protect" it or pay a fine that way | Any real issue is handled through official channels - not a convenience-store kiosk

Secrecy and coaching | Stay on the phone; do not tell family or your bank; follow their QR and machine directions | Encourages you to use your own verified contacts; does not coach a secret cash dump | A second trusted person or your bank's published number breaks the script

Safe next step | Hang up; do not withdraw cash; do not scan their QR at any kiosk | Still verify yourself on a number from your statement or official site | If nobody confirms the story, treat the original call as a scam and report it

How to spot a Bitcoin ATM cash deposit scam

Run this kiosk-focused checklist before you leave with cash or scan a machine code.

* Treat any "go to a Bitcoin ATM" instruction as a scam signal. The FTC's March 2024 alert says there is no legit reason for someone to send you to a Bitcoin ATM, and government never will. The September 2024 alert says real businesses and government agencies will never tell you to use a BTM to protect money or fix a problem.

* Never withdraw cash because of an unexpected call or message. Both the September 2024 consumer alert and the Data Spotlight say only scammers tell you to do that. If the person on the line needs you at an ATM with a stack of bills, hang up before you leave the house.

* Refuse QR codes texted for a kiosk deposit. The Data Spotlight and September 2024 press release describe scammers texting a QR code so scanned deposits land in their wallet. A QR from an unexpected caller is not a "government deposit address" or a "safety locker" key - the March 2024 alert says those lockers do not exist.

* Verify the story yourself on a number or site you already trust. The September 2024 alert says if you think there is a real problem with an account, use a phone number, website, or app you know is real. The March 2024 alert says to reach your real bank, broker, or investment advisor through the contact printed on account statements - never through the callback the caller dictates. The FBI PSA says to ask for credentials and verify through official, publicly available contacts.

* Break the stay-on-the-phone rule. The FBI PSA warns that scammers keep victims on the line and urge secrecy from family and banks. Put the phone down, talk to someone you trust, and call your bank from a second device if needed.

Secrecy plus a kiosk QR is the scam working as designed.

* Log the attempt even when you walked away empty-handed. Open [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud) (How to report a scam to the FTC) for the FTC side. For impersonation plots, [IC3.gov](https://www.ic3.gov) wants your contact details, payment or cryptocurrency clues, and messages that carried QR codes - file there too. Empty-handed stops still help investigators.

Low-cost habits that block kiosk coaching

None of these needs a paid subscription.

* Household rule: nobody withdraws cash, buys gift cards, or moves money to "protect" an account because an unexpected caller said so. Gift-card pressure is a related channel - see the gift card scam guide if that is what they demanded instead of a kiosk.

* Know what a Bitcoin ATM looks like in a store or gas station versus a bank ATM that only dispenses your own cash. If someone on the phone is directing you to the crypto machine, that is your cue to leave.

* Save your bank's, brokerage's, and major account providers' customer-service numbers from statements or official apps so a panic call never becomes your only contact path.

* If a relative calls in panic about an arrest or warrant and payment must be cash at a crypto kiosk, hang up and verify with them another way - and treat jury-duty or warrant scripts as their own patterns in the jury duty / warrant scam guide rather than a reason to visit a BTM.

* Keep email and banking behind unique passwords in a password manager, with multi-factor authentication on (Password manager setup for a US household | Turn on 2FA for Gmail, Apple, and your bank).

* Bookmark [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud) and [IC3.gov](https://www.ic3.gov) yourself so a panicked caller never becomes your reporting channel.

* Save any QR text, machine location, and receipt only for your bank and police report - never to finish a coached deposit.

Related scams this page skips

Scope here is narrow: surprise contact that pushes you to take cash out and feed a Bitcoin ATM or crypto kiosk - usually after a texted QR - with a "protect the money," fake account crisis, or fake government/bail story.

For fake trading apps and investment pitches, use the cryptocurrency scam guide. Giveaway bait belongs in Discord Nitro crypto giveaway scam. If the demand was cards, wires, or P2P apps instead of a kiosk, jump to gift card scam, wire transfer romance / advance-fee scam, or Zelle / Cash App payment scam. Pop-up remote-access openers live in tech support scam phone call; this article starts at the cash-to-machine step. Script-focused pages - Social Security scam, jury duty / warrant scam, fake IRS tax refund scam - cover those impersonation stories; here the payment channel is the BTM. Filing walkthrough: How to report a scam to the FTC. Voluntary personal crypto purchases at a kiosk are outside this warning, and nothing here replaces legal advice beyond the cited FTC and FBI pages.

Compare antivirus plans only if you already want them

Nothing below is required to refuse a coached BTM deposit. If you later decide to shop device or identity suites on your own timeline, these on-site product pages are the only paid links on this guide:

* Norton plans: look at device protection tiers that also bundle identity tools on some plans ([paid link](#); check renewal pricing before you buy).

* Bitdefender plans: useful to compare if you care about independent lab rankings more than brand familiarity ([paid link](#)).

* TotalAV plans: a multi-device household option to price against other suites ([paid link](#); confirm what renews).

* McAfee plans: one subscription covering several devices for households that want a single bill ([paid link](#); check the device cap).

* Avast plans: another suite some homes already run and may prefer to keep ([paid link](#)).

You can skip every paid option. These links stay on this site only.

FAQ

Is there any legitimate reason for someone to send me to a Bitcoin ATM?

No. The FTC's March 2024 consumer alert says the short answer is no, and government will never send you to a Bitcoin

ATM. Anyone who claims a BTM will protect your money or fix a problem is a scammer, according to the September 2024 alert.

What is a "safety locker" in these calls?

It is a scam label. The FTC's March 2024 alert says there are no Bitcoin federal safety lockers and no government Bitcoin account. The September 2024 Data Spotlight notes that scammers have called Bitcoin ATMs "safety lockers" while directing victims to deposit cash.

Why do they text a QR code?

So the cash you insert is credited to their wallet. The FTC Data Spotlight and September 2024 press release describe scammers texting a QR code to scan at the machine; once you do, the deposit goes to them. Do not scan it.

Can a tech support or government story still end at a Bitcoin ATM?

Yes. The Data Spotlight says BTM fraud reports are overwhelmingly tied to government impersonation, business impersonation, and tech support scams. The story brand can change; the stop sign is still "withdraw cash and feed this kiosk." For the pop-up path, see the tech support scam phone call guide; for Social Security or warrant scripts, see those guides listed under "Related scams this page skips."

What should I do if I already deposited cash?

Tell the bank desk that answers on the printed statement line or inside the official app that a caller steered you into a BTM. Preserve the kiosk receipt, store location, and QR text for police. Submit [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud), then [IC3.gov](https://www.ic3.gov), as two separate filings. Recovery is often difficult once crypto moves, which is why the FTC stresses not withdrawing cash first.

I already sent money another way or shared account details. What now?

Use only bookmarked or statement-printed contacts for the bank, wire firm, or payment app, and ask which freezes or reversals are still possible. File [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud) first, then [IC3.gov](https://www.ic3.gov). If personal information was misused, start at [IdentityTheft.gov](https://www.identitytheft.gov) (Report identity theft). Related payment checklists: gift card scam, wire transfer romance / advance-fee scam, and Zelle / Cash App payment scam.

Sources

- * Scammers use Bitcoin ATMs to steal your money (FTC Consumer Advice, Sep 3, 2024)
- * Did someone send you to a Bitcoin ATM? It's a scam (FTC Consumer Advice, Mar 7, 2024)
- * Bitcoin ATMs: A payment portal for scammers (FTC Data Spotlight, Sep 3, 2024)
- * New FTC Data Shows Massive Increase in Losses to Bitcoin ATM Scams (FTC press release, Sep 3, 2024)
- * Scammers Impersonating Law Enforcement and Government Officials in Fraud Schemes (FBI IC3 PSA, Sep 17, 2026)
- * [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)
- * [IdentityTheft.gov](https://www.identitytheft.gov)
- * Internet Crime Complaint Center (FBI IC3)

Also read

- * Cryptocurrency scams
- * Social Security scams
- * Fake IRS tax refund scams
- * Discord Nitro crypto giveaway scams