BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Crypto & Bitcoin ATM Scams

What crypto machines are, how scammers use them, and what to do — explained in plain English, one step at a time

A plain-English guide for seniors and families

Nobody real ever sends you to a Bitcoin machine

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

Crypto ATMs, crypto basics and the scams that use them · facts current November 2026

What's Inside

This is your guide to crypto ATMs and the scams that send people to them. Start with the one rule in Part 1. Part 2 explains crypto in plain words, Part 3 shows how the scams work, and Part 4 is the step-by-step plan if money has already gone. Read in any order and at your own pace.

Part 1 — Start Here

1 A Note from Bill
2 The One Rule That Stops Every Crypto ATM Scam
3 Is Someone Pushing You to a Bitcoin Machine Right Now?
4 Why Scammers Love Crypto ATMs
5 The Numbers: What the FTC and FBI Report

Part 2 — Crypto in Plain English

6 What Is Cryptocurrency?
7 Wallets and Addresses, Explained
8 What Is a Blockchain, and Why Payments Can't Be Undone
9 What a Crypto ATM Looks Like and Where You'll See One
10 How a Crypto ATM Transaction Actually Works
11 QR Codes: The Scammer's Shortcut
12 Crypto Is Not a Bank Account
13 If You Choose to Own Crypto: What to Avoid

Part 3 — How the Scams Work

14 The Scam Script: Five Steps Most Crypto ATM Scams Follow
15 Fake Tech Support and the Frozen Computer
16 The Fake Bank "Fraud Department"
17 Government Impostors: IRS, Social Security, Police and the FBI
18 The "Phantom Hacker" Three-Act Scam
19 Romance Scams That End at a Bitcoin Machine
20 "Pig Butchering": Fake Crypto Investment Apps
21 Family Emergency, Utility, Prize and Job Scams
22 Red Flags at a Glance

Part 4 — If You Already Paid

23 If You Already Put Money in a Bitcoin Machine
24 Your Receipt and Notes Are Evidence
25 Call the Kiosk Company and Your Bank
26 Report It: FBI, FTC and Local Police
27 Ohio Help and Ohio's Crypto Kiosk Rules

28 Recovery Scams: The Second Hit
29 The Emotional Side, and Talking With Family

Part 5 — Protecting Yourself & Your Family

30 Your Scam Pause Plan
31 Helping a Parent or Loved One
32 Questions People Ask About Crypto ATMs
33 When to Call Bill
34 Your Crypto Scam Cheat-Sheet

PART 1

Start Here

The one rule that stops every Bitcoin ATM scam, what to do if someone is pushing you toward a machine right now, and why scammers have fallen in love with these machines.

CHAPTER 1

A Note from Bill

Hello, and welcome. You may have noticed a new kind of machine in the corner of a gas station or convenience store. It looks a lot like a bank ATM, but it says **Bitcoin** or **Crypto** on the front. Most people walk right past it. Scammers, unfortunately, have found a use for it: it's one of the fastest ways for them to turn your cash into money they can grab and never give back.

I'm Bill. For more than 30 years I've helped people make sense of their technology, and I serve folks right here in Portage County, Ohio. I wrote this guide the way I'd explain it at your kitchen table: slowly, in plain English, with no lecture and no jargon left unexplained.

Who this guide is for

- Anyone who has never touched cryptocurrency and wants to understand what it is, in plain words.
- Anyone who got a call, text, pop-up or message telling them to take cash to a Bitcoin machine.
- Anyone who **already put money in a Bitcoin machine** and wants to know what to do now.
- Grown children and caregivers who want to protect a parent, with that parent's blessing.

WHAT THIS DOES FOR YOU

What this guide does for you

By the end you'll know what a crypto ATM is and how it works, the handful of scripts scammers use to send people to one, the warning signs that give them away, and exactly who to call if money has already gone. You'll also learn enough crypto basics to never feel talked down to again.

An honest promise

In most of my guides I tell you that you can't break anything by exploring. This topic is different: money put into a crypto machine usually can't be pulled back. So I'll be plain and a little firm. **Reading this guide costs nothing and risks nothing.** The only risky step is feeding cash into a machine because someone told you to, and by the end of Chapter 2, *The One Rule That Stops Every Crypto ATM Scam* you'll know never to do that.

If you're reading this because it already happened, please hear this first: **it is not a sign that you're foolish.** These scams are run by organized crews who do this all day. Jump to Chapter 23, *If You Already Put Money in a Bitcoin Machine* and take it one step at a time. If you'd like the broader first-day plan for any kind of scam, my guide *I Think I've Been Scammed* walks through it, and *Spotting and Avoiding Scams* covers the tricks beyond crypto.

You're never stuck alone

If anything here feels like too much, or someone is on the phone with you right now, hang up and call or text me at **(330) 200-8042**. I'd much rather spend two minutes reassuring you than have you lose a dime.

— Bill

CHAPTER 2

The One Rule That Stops Every Crypto ATM Scam

If you remember nothing else from this guide, remember this one sentence. It works every single time, no matter how convincing the caller sounds.

SCAM ALERT

The rule

Anyone who tells you to put money into a Bitcoin ATM or crypto kiosk is a scammer. Not sometimes. Every time. No real bank, government agency, police department, utility, tech company or loved one in trouble will ever send you to one of these machines.

Why the rule is so simple

The Federal Trade Commission (FTC), the federal agency that fights scams, puts it bluntly: only scammers demand payment in cryptocurrency. No legitimate business is going to demand that you send cryptocurrency in advance, whether to buy something or to "protect" your money. The FBI says the same thing about the government: no real law enforcement or government official will call and demand payment through a cryptocurrency kiosk.

Words that mean the same thing

Scammers use different names so the instruction sounds new. All of these are the same machine, and the same rule applies to each one:

- Bitcoin ATM, or BTM
- Crypto ATM, or cryptocurrency ATM
- Crypto kiosk, virtual currency kiosk, or digital currency kiosk
- "The machine at the gas station" or "the kiosk at the store"

The rule has a cousin

The same logic covers the other favorite scam payments. If anyone insists you pay with **gift cards**, a **wire transfer**, **cash handed to a courier**, or **crypto**, stop. Those payment methods are chosen because they are fast and very hard to undo, not because any real organization needs them.

TIP

Say it out loud

Some people find it helps to write the rule on a sticky note by the phone: *"Nobody real sends me to a Bitcoin machine."* When a caller is pushing hard, reading your own handwriting can break the spell.

CHAPTER 3

Is Someone Pushing You to a Bitcoin Machine Right Now?

If you're reading this with a caller still on the line, a pop-up on your screen, or a text telling you to hurry, this chapter is for you. Do these things in order. None of them can hurt you.

1. **Hang up**, or stop replying. You don't owe the caller an explanation. If they called you, you can end the call.
2. **Do not go to the bank, the store or the machine.** If you're already standing at a kiosk, step away from it. If the screen is in the middle of a purchase, don't insert any more cash.
3. **If your computer showed a scary warning,** don't call the number on it. Turn the computer off with the power button.
4. **Call someone you trust** on a number you already know: a family member, your bank (the number on the back of your card), or me at (330) 200-8042.
5. **Write down** the phone numbers, names and anything they told you, while it's fresh. Don't delete the texts or emails yet.

> STAY SAFE
>
> **If anyone says they're coming to your home for cash**
>
> Don't open the door, and call 911. Some crews send a "courier" to collect cash or valuables in person. A real agency never does this.

What the caller will say to keep you on the line

Scammers know that the moment you talk to someone else, the scam falls apart. So they'll try to stop you. Recognize these lines for what they are:

If they say…	What's really going on
"Don't tell the bank teller why you're withdrawing."	A real investigator never asks you to lie to your bank. This line alone proves it's a scam.
"Stay on the phone the whole time."	They want to stop you from thinking or calling anyone. Hang up.
"This is confidential. You'll be arrested if you tell anyone."	Threats and secrecy are the scammer's tools, not the law's.
"The store clerk is part of the fraud. Don't talk to them."	Clerks and kiosk companies sometimes try to warn people. Listen to them.

HEADS UP

If the machine itself warns you

The FBI's advice is simple: if a kiosk operator warns that your transaction looks like fraud, stop or cancel the transaction. Those warnings are there because the company has seen this exact story before.

When you're safe and calm, come back and read Chapter 14, *The Scam Script: Five Steps Most Crypto ATM Scams Follow* to see how the whole trick fits together.

CHAPTER 4

Why Scammers Love Crypto ATMs

Scammers have used gift cards and wire transfers for years. Crypto machines give them something even better. Understanding why helps the rule stick.

Four reasons crooks choose these machines

Reason	What it means for you
Cash goes in, crypto goes out in minutes	You feed paper money into the machine and it is converted and sent almost right away. There's no waiting period for anyone to notice.
Payments usually can't be reversed	The FTC notes that crypto payments don't have the same legal protections as credit or debit cards, and usually can't be undone once sent.
The money goes to a "wallet," not a name	Crypto is sent to a long code called a wallet address. The person behind it doesn't have to be standing anywhere near you.
Machines are everywhere	They sit in busy, everyday places, so a scammer can always send you to one a few minutes away.

Why the scam starts somewhere else

Here's the clever part. Nobody gets scammed *by* the machine. The scam starts with a phone call, a text, an email, a pop-up on your computer, or a new friend online. The machine is just the last step: the cash register the crook uses to collect. That's why this guide spends so much time on the stories that lead people there. See Chapter 14, *The Scam Script: Five Steps Most Crypto ATM Scams Follow*.

GOOD TO KNOW

Good to know: the machines themselves are legal

Crypto ATMs are legal businesses, and some people use them on purpose to buy cryptocurrency. This guide isn't about whether you should ever own crypto. It's about one thing: **never using one because someone else told you to.**

The federal government has noticed

In August 2025, FinCEN, the part of the U.S. Treasury that watches for financial crime, issued a notice warning banks and other financial institutions about scams and other illegal activity at crypto kiosks, including tech support scams and fake bank "fraud department" calls. In other words, this isn't a rare trick; it's on the radar of federal regulators.

CHAPTER 5

The Numbers: What the FTC and FBI Report

I don't use scare statistics lightly, and I only use numbers that the government itself published. These come straight from the FTC and the FBI. Every agency says the same thing about them: they count only what people reported, so the real losses are likely higher.

What the FTC found (published September 2024)

- Reported losses to Bitcoin ATM scams grew nearly **tenfold** from 2020 to 2023, reaching more than **$110 million in 2023**.
- In just the first six months of 2024, reported losses topped **$65 million**.
- People **60 and over** were more than **three times as likely** as younger adults to report losing money this way. They reported losing about $46 million in that half-year, roughly 71% of the total.
- The median reported loss in the first half of 2024, across all ages, was **$10,000**.
- Most of the losses came from **government impersonation, business impersonation and tech support scams**.

What the FBI found (2024 and 2025 complaints)

Year	Complaints to the FBI about crypto kiosks	Reported losses
2024	10,956	About $246.7 million
2025	More than 13,400	More than $388 million

The FBI's Internet Crime Complaint Center (IC3) reported that 2025 brought a 23% rise in complaints and a 58% rise in losses compared with 2024. More than half of the 2025 complaints involved people over 50, with losses over $302 million. The FBI adds a fair caveat: some of these complaints may include other kinds of transactions too, so not every dollar can be blamed on the kiosk alone.

GOOD TO KNOW

What the numbers mean for you

These aren't numbers to frighten you. They're the reason the one rule in Chapter 2, *The One Rule That Stops Every Crypto ATM Scam* matters so much. The FTC's figures show older adults are hit hardest. Being polite on the phone is a virtue; with these callers, hanging up is the kind thing to do for yourself.

The bigger crypto picture is even larger. The FBI reported that cryptocurrency investment fraud was the single biggest source of reported losses to Americans in 2025, at about $7.2 billion. That's the kind of scam covered in Chapter 20, *"Pig Butchering": Fake Crypto Investment Apps*.

PART 2

Crypto in Plain English

What cryptocurrency is, how wallets and blockchains work, what a crypto ATM looks like and how it works, and why crypto is not like money in the bank. No investment advice, just plain words.

CHAPTER 6

What Is Cryptocurrency?

You don't need to understand crypto to stay safe from crypto scams; the rule in Chapter 2, *The One Rule That Stops Every Crypto ATM Scam* is enough. But a little understanding takes the mystery away, and mystery is what scammers count on. So here's the kitchen-table version.

The short answer

Cryptocurrency is digital money that isn't issued by a government or kept by a bank. It exists only as records on computers spread around the world. There are no coins or bills. When people say they "own Bitcoin," they mean a public record shows that a certain amount belongs to a code that only they control.

A few names you'll hear

Name	What it is
Bitcoin	The first and best-known cryptocurrency, started in 2009. It's the one most crypto ATMs sell, which is why they're often called Bitcoin ATMs.
Ethereum, Litecoin and others	Other cryptocurrencies. Thousands exist. Some machines sell several.
Stablecoins (such as USDT or USDC)	Crypto designed to stay worth about one dollar each. Scammers like these too, because the amount doesn't wobble while they're collecting it.
Crypto, coins, tokens, digital currency	Everyday words that all mean roughly the same thing.

How crypto is different from dollars in the bank

	Money in your bank	Cryptocurrency
Who keeps the records	Your bank	A shared public record on many computers
If you're tricked into a payment	Often a dispute process, depending on how you paid	Usually no way to reverse it
Insured by the FDIC	Yes, up to the legal limits at insured banks	No
Value	A dollar stays a dollar	Can rise or fall sharply, even in a single day
Someone to call	Your bank's fraud line	Often no one who can undo anything

GOOD TO KNOW

No investment advice here

This guide doesn't tell you whether to buy crypto. That's a money decision for you and a trusted financial advisor. My job is to explain the words and keep you away from the scams.

CHAPTER 7

Wallets and Addresses, Explained

When a scammer sends you to a machine, they always give you something called a **wallet address**, usually as a QR code. Knowing what that is shows you exactly where your money is going.

What a crypto "wallet" is

A crypto wallet isn't a leather wallet and it doesn't hold coins. It's more like a **mailbox with a special key**. Anyone who knows the mailbox number can drop money in. Only the person with the key can take money out. A wallet can live in a phone app, on a website, or on a small device.

Word	What it means
Wallet address	The mailbox number. A long string of letters and numbers. You can give it out to receive crypto. Scammers give you *theirs*.
Private key or recovery phrase	The key to the mailbox. Often a list of 12 or 24 ordinary words. Whoever has it controls everything in the wallet. Never share it with anyone.
QR code	A square barcode that holds the wallet address, so nobody has to type that long string.
Transaction ID (sometimes TXID or hash)	A receipt number for one payment on the blockchain. Useful when you report a scam.

SCAM ALERT

If anyone asks for your recovery phrase

It's a scam, full stop. A real crypto company, app or support agent never needs your recovery phrase or private key. Giving it out is like handing over your house keys and your alarm code at once.

The key point about a scammer's wallet address

When a caller sends you a QR code and says it's "your safe account," "a government wallet" or "the bank's secure vault," what they've really sent is **their own mailbox number**. The money goes to the scammer the moment it's sent. There is no such thing as a government or bank "safe wallet" you deposit cash into at a gas station.

TIP

Your own wallet, if you ever have one

If you ever decide to own crypto, set up the wallet yourself, from the official app store, with no one on the phone telling you what to tap. Write the recovery phrase on paper and keep it somewhere safe, away from your phone.

CHAPTER 8

What Is a Blockchain, and Why Payments Can't Be Undone

You'll hear the word **blockchain** a lot. It sounds technical, but the idea is simple, and it explains why crypto scams hurt so much.

The plain-English version

Picture a giant shared ledger book, copied onto thousands of computers around the world. Every crypto payment is written into that ledger as a new line. Once enough computers agree that a line is correct, it's sealed in, in a "block," and the blocks are linked together in a "chain." Nobody can go back and erase a line. That's the blockchain.

What that means when you're tricked

- There's no bank in the middle that can freeze or claw back a payment the way a credit card company can.
- Once the payment is confirmed, it's permanent. The FTC says crypto payments usually can't be reversed.
- The ledger is public, so investigators can sometimes trace where money went. That's why reporting it matters, even when you can't get it back yourself. See Chapter 26, *Report It: FBI, FTC and Local Police*.

> **GOOD TO KNOW**
>
> **"Public" doesn't mean "named"**
>
> The ledger shows wallet addresses and amounts, not people's names. That's part of why scammers like it. Law enforcement has tools to follow the trail, but it takes time and isn't a promise of getting money back.

Why scammers rush you

Because crypto can't be undone, the scammer's whole job is to get you to the machine before you talk to anyone. That's why every crypto ATM scam comes with a deadline: "in the next hour," "before the bank closes," "before the warrant is served." **Real problems can wait for you to make a phone call. Scams can't.**

CHAPTER 9

What a Crypto ATM Looks Like and Where You'll See One

Knowing what the machine looks like helps you recognize the moment a story is heading there. If a caller directs you to a store and starts describing one of these, you'll know.

What it looks like

- It looks a lot like a regular bank ATM: a tall cabinet with a touch screen.
- It usually has a slot for **inserting** cash, because most of these machines take cash in rather than giving cash out.
- It has a **camera or scanner** to read a QR code from a phone or a piece of paper.
- The front or screen shows a company name and a word like **Bitcoin**, **BTC**, **Crypto** or **Digital Currency**.
- Many print a paper receipt at the end.

Where you'll find them

The FTC describes them as being placed in high-traffic locations. In everyday terms, that often means convenience stores, gas stations, and similar busy shops, the kind of place you can drive to in a few minutes from almost anywhere, including here in Portage County.

SCAM ALERT

"Go to the one at this address"

The FTC found that scammers often send people to a specific machine at a specific location, and stay on the phone while they drive there. A caller who knows which store has a Bitcoin machine near your house is not your bank and not the government.

How it's different from a bank ATM

Machine	What it does
Bank ATM	Run by or for your bank. Takes your bank card. Gives you cash from your own account.
Crypto ATM	Run by a private crypto company. Takes your cash. Sends crypto to whatever wallet address you scan or type in, which may belong to anyone.

TIP

Seeing one is not a reason to worry

The machine sitting in the store isn't dangerous on its own. Walk past it like you'd walk past a lottery ticket machine. It only becomes a problem when someone else is telling you to use it.

CHAPTER 10

How a Crypto ATM Transaction Actually Works

I'm explaining these steps so you'll recognize them, not so you'll follow them. If anyone ever walks you through this list on the phone, you are talking to a scammer.

What happens at the machine

1. The person taps the screen to start a purchase and picks a cryptocurrency, usually Bitcoin.
2. The machine may ask for a phone number, a code sent by text, or a photo ID, depending on the company and the amount.
3. The machine asks where to send the crypto. The person holds up a **QR code** to the scanner. That QR code is the destination wallet address.
4. The person feeds cash into the slot, one bill at a time. The screen counts it up.
5. The person confirms. The machine sends the crypto to the wallet in the QR code and prints a receipt.

Where the scam hides in those steps

Look at step 3. Whoever made that QR code owns the money the instant the purchase is complete. In a scam, the caller texted or emailed that QR code to you beforehand, or told you to print it. You aren't depositing money into any account of yours. You're buying crypto and handing it to a stranger.

> HEADS UP
>
> **Watch for "do it in pieces"**
>
> Scammers often tell people to split the cash across several trips or several machines, or to go back the next day, so the amounts stay under a machine's limits. Being told to break up a payment is another clear sign of a scam.

Fees and limits

Crypto ATM companies charge for the service, and the screen and receipt show what was charged. Many machines also have daily limits on how much cash they'll take, which is part of why scammers send people back again and again. Some states have passed laws capping those limits; see Chapter 27, *Ohio Help and Ohio's Crypto Kiosk Rules* for where Ohio stands.

GOOD TO KNOW

The receipt matters

If money has already gone in, the paper receipt is one of the most important things you have. It shows the amount, the date and time, and usually the wallet address. Keep it. See Chapter 24, *Your Receipt and Notes Are Evidence*.

CHAPTER 11

QR Codes: The Scammer's Shortcut

QR codes are the little black-and-white squares you scan with a phone camera. They're handy and mostly harmless: restaurant menus, parking meters, product manuals. In crypto ATM scams, though, the QR code is the scammer's address label.

How the QR code trick works

The FTC describes it this way: the scammer sends you a QR code with their wallet address embedded in it. Once you buy the cryptocurrency at the machine, they have you scan that code, and the money is transferred to them. You never see the long address, so you never realize it isn't yours.

Red flags involving QR codes

- Someone texts, emails or mails you a QR code and tells you to scan it at a machine.
- You're told to print a QR code and bring it to a store.
- You find yourself holding QR code papers you can't explain or didn't make yourself. The FBI lists this exact situation as a warning sign.
- A caller says the QR code is "your secure account" or "the government's wallet."

SCAM ALERT

Never scan a payment QR code a stranger sent you

The simple version: if someone else gave you the QR code, the money goes to someone else. There's no other way it works.

TIP

For families

If you're helping a parent and you find printed QR codes, wallet addresses, or Bitcoin ATM receipts among their papers, don't scold. Ask gently what they're for. It may be the first sign of a scam that's still going on. See Chapter 31, *Helping a Parent or Loved One*.

CHAPTER 12

Crypto Is Not a Bank Account

Some scams work because people assume crypto has the same safety nets as their bank account. It doesn't. Knowing the differences takes away the scammer's best lines.

Three safety nets crypto doesn't have

Missing safety net	What it means
No FDIC insurance	The FDIC protects deposits at insured banks. It does not cover crypto, and it doesn't protect you if a non-bank crypto company fails.
No government insurance at all	The CFPB has noted that no government agency or financial regulator insures crypto-assets.
No easy undo	Credit cards come with dispute rights. Crypto payments generally don't have those same legal protections and usually can't be reversed.

Values can swing wildly

The CFPB has warned that crypto values have swung, and will likely keep swinging, a great deal. A coin worth a certain amount on Monday can be worth much less by Friday. That's normal for crypto, and it's one more reason it's a poor place to "keep money safe."

SCAM ALERT

"Move your savings into crypto to protect it"

This is one of the most common scam lines. Your bank, the FTC, the FBI and the Social Security Administration will never ask you to protect your savings by turning them into crypto. Crypto is the opposite of protected.

If you hear "it's FDIC-insured"

Some fake crypto sites and apps claim to be FDIC-insured or government-backed. The FDIC has said its insurance doesn't cover crypto assets. A claim like that is a reason to walk away, not a reason to trust.

CHAPTER 13

If You Choose to Own Crypto: What to Avoid

Some people decide to own a little crypto on purpose, for their own reasons. That's your choice, and this guide won't tell you yes or no. But whether you own it or not, a few habits keep you out of the traps that catch people every day.

Things to avoid, always

1. **Never buy crypto because someone else told you to,** especially someone you met online or who contacted you first.
2. **Never share your recovery phrase or private key,** with anyone, for any reason.
3. **Never let anyone "help" you set up a wallet** over the phone, by remote access, or on a video call.
4. **Never download a trading app from a link** someone sent you. Fake apps and websites are a big part of investment scams. See Chapter 20, *"Pig Butchering": Fake Crypto Investment Apps*.
5. **Never pay "taxes" or "fees" to withdraw your money.** The FBI lists this as a top sign of a fake platform.
6. **Be wary of promises of guaranteed or high returns.** No honest investment can promise that.

Before you invest in anything crypto-related

Talk it over with someone you trust who has nothing to gain: a family member, your banker, or a licensed financial advisor you chose yourself. A good test: if you'd be embarrassed to tell your family about an investment, or the person pitching it asked you to keep it secret, that's your answer.

> **GOOD TO KNOW**
>
> **A machine is not where people usually start**
>
> People who buy crypto for themselves typically use an account they opened on their own. A crypto ATM visit that someone else arranged for you is a very different thing. If the idea came from a caller, text or online friend, see Chapter 2, *The One Rule That Stops Every Crypto ATM Scam*.

FROM BILL

I'm happy to look

If someone has pitched you a crypto opportunity and you want a second set of eyes, call me at (330) 200-8042 before you send anything. I won't give investment advice, but I can tell you whether the website, app or story has the marks of a scam.

PART 3

How the Scams Work

The stories that send people to a Bitcoin machine: fake tech support, the bank "fraud department," government impostors, romance, fake investment apps and more, and the warning signs they share.

CHAPTER 14

The Scam Script: Five Steps Most Crypto ATM Scams Follow

The costumes change, but the play is almost always the same. Once you see the script, you'll recognize it no matter who the scammer pretends to be.

1. **The scare or the lure.** A call, text, email, pop-up or new online friend. Something is wrong with your account, your computer, your Social Security number, or there's an amazing opportunity.
2. **The "expert."** You're passed to someone who sounds official: a bank fraud investigator, a Microsoft technician, a federal agent, a successful investor.
3. **The secret.** You're told not to tell anyone, not even the bank teller or your family, because "they might be involved" or "it's a confidential investigation."
4. **The cash.** You're told to withdraw cash, often a large amount, sometimes in several trips.
5. **The machine.** You're sent to a specific Bitcoin ATM and given a QR code to scan. The money goes to the scammer.

SCAM ALERT

Any one step is enough to stop

You don't need to figure out which scam it is. The moment you hear "keep this secret," "withdraw cash," or "Bitcoin machine," you have your answer. Hang up and call someone you trust.

The most common costumes

The FTC found that most Bitcoin ATM losses came from three kinds of impostors: **government impersonators**, **business impersonators** (often your bank, Amazon or a tech company) and **tech support** scammers. Romance and fake investment scams also end at these machines. The next chapters take each one in turn.

Costume	Read more
Fake tech support	Chapter 15, *Fake Tech Support and the Frozen Computer*
Fake bank fraud department	Chapter 16, *The Fake Bank "Fraud Department"*
Government impostor	Chapter 17, *Government Impostors: IRS, Social Security, Police and the FBI*

Costume	Read more
The three-act "phantom hacker"	Chapter 18, *The "Phantom Hacker" Three-Act Scam*
Romance	Chapter 19, *Romance Scams That End at a Bitcoin Machine*
Fake crypto investment	Chapter 20, *"Pig Butchering": Fake Crypto Investment Apps*
Family emergency, utility, prize and job	Chapter 21, *Family Emergency, Utility, Prize and Job Scams*

CHAPTER 15

Fake Tech Support and the Frozen Computer

This one often starts while you're minding your own business on the computer. Suddenly the screen is covered with a loud warning, maybe a siren sound, saying your computer is infected or your bank account has been hacked, and to call a number right away.

How it usually goes

1. A pop-up claims to be from Microsoft, Apple, or a security company. It shows a phone number.
2. You call. A friendly "technician" asks to connect to your computer to "check it."
3. Once connected, they show you scary-looking screens and say hackers have reached your bank or that your money is being used for crimes.
4. They transfer you to your "bank" or a "government agent" who tells you to move your money to keep it safe, by withdrawing cash and depositing it at a Bitcoin ATM.

STAY SAFE

What to do instead

Don't call the number on a pop-up. Close the browser, or turn the computer off with the power button if it won't close. Real Microsoft and Apple warnings don't come with a phone number to call, and real companies don't tell you to buy crypto.

If you already let them connect

- Turn the computer off or disconnect it from the internet.
- Call your bank on the number on the back of your card and tell them what happened.
- From a different device, change the passwords for your email and bank.
- Have the computer checked. My guide *Remote Support and Fake Tech Support* walks through it, and I can help too.

GOOD TO KNOW

The pop-up isn't a virus, usually

Most of these scary screens are just a web page made to look like a warning. Closing the browser often makes it go away completely. My guide *Pop-Ups and Fake Virus Alerts* shows how to close one safely.

CHAPTER 16

The Fake Bank "Fraud Department"

This scam borrows the trust you have in your bank. The call or text looks like it's from your bank's fraud team, and the caller ID may even show the bank's real name or number. Caller ID can be faked.

How it usually goes

1. A text asks whether you made a large purchase. You reply "no," or you get a call a moment later.
2. The "fraud department" says criminals are draining your account, or that a bank employee is in on it.
3. To "protect" your money, they say you must withdraw cash and move it to a "safe account."
4. The safe account turns out to be a Bitcoin ATM and a QR code they send you.

SCAM ALERT

Your bank will never do this

No real bank will ever tell you to withdraw cash to protect it, move money to a "safe account," or deposit cash into a crypto machine. The FTC advises calling your bank yourself, using the number on your statement or the back of your card, not the number the caller gives you.

How to check a call that claims to be your bank

1. Say, "I'll call the bank back myself," and hang up. A real bank employee will understand.
2. Wait a minute. Scammers sometimes stay on the line after you hang up, so if you can, use a different phone, or wait before dialing.
3. Call the number printed on the back of your bank card or on your statement.
4. Ask, "Is there any problem with my account? Did anyone from your fraud team just call me?"

TIP

If the bank teller asks questions, it's a good thing

Tellers are trained to notice when someone is withdrawing a large amount in a hurry. If a teller asks why you need the cash, tell them the truth. They're on your side, and it's the scammer who told you to lie.

CHAPTER 17

Government Impostors: IRS, Social Security, Police and the FBI

Government impostors are among the biggest sources of Bitcoin ATM losses. They lean on fear: arrest, frozen benefits, a stolen identity, a warrant. They may know your name and address, and they may send pictures of badges or official-looking letters.

Lines you might hear

- "Your Social Security number was used in a crime. Your benefits will be suspended."
- "There's a warrant for your arrest for missing jury duty. Pay the fine now."
- "You owe back taxes and will be arrested today."
- "This is the FBI (or the FTC). Your money is evidence. Move it to a government wallet to protect it."

SCAM ALERT

No agency takes payment through a crypto machine

The FBI says no legitimate law enforcement or government official will call to demand payment via a cryptocurrency kiosk, and that officials never demand payment by phone or text through prepaid cards, crypto or a courier. The FTC agrees: nobody from the government, law enforcement or a utility will ever tell you to pay with cryptocurrency.

They may even show up on video

In a September 2026 warning, the FBI said impostors now use look-alike websites and even AI to appear as officials on video calls. Seeing a uniform or badge on a screen proves nothing. The rule doesn't change: a real official never sends you to a Bitcoin machine.

How to check

1. Hang up. Don't use any number the caller gives you.
2. Look up the agency's number yourself, on a letter you already have or on the agency's official website, or call your local police non-emergency number.
3. Ask whether there's really a problem. There almost never is.

CHAPTER 18

The "Phantom Hacker" Three-Act Scam

The FBI has named one especially convincing version the "phantom hacker" scam. It's a team effort: three different impostors, each one handing you to the next, so every call seems to confirm the last.

Act	Who calls	What they say
1	Fake tech support	Your computer was hacked. Let me check whether your accounts are safe.
2	Fake bank	A foreign hacker is in your account. Move your money somewhere safe.
3	Fake government agent	Your money is at risk. Put it in this protected account (often a Bitcoin ATM, a wire, or cash to a courier).

Because three "different" organizations agree with each other, it feels real. They're the same crew, passing you down the line.

SCAM ALERT

The giveaway

No real agency, bank or tech company works together to have you move your own money. The moment the conversation turns to moving savings, it's a scam, no matter how many people have "confirmed" it.

What to do

- Stop all contact. Don't call back any number they gave you.
- Call your bank on the number on your card.
- Have a trusted person or a technician check the computer if the scammers connected to it.
- Report it at **ic3.gov**. See Chapter 26, *Report It: FBI, FTC and Local Police*.

GOOD TO KNOW

Why they take their time

These crews may call over days or weeks, building trust. Some move from Bitcoin ATMs to sending a courier for cash or gold. If anyone ever offers to send someone to pick up money, it's the same scam.

CHAPTER 19

Romance Scams That End at a Bitcoin Machine

Romance scams don't start with fear. They start with kindness. Someone you meet on a dating site, Facebook, a game, or by a "wrong number" text becomes a warm, attentive friend. Weeks or months later, they need money, and crypto is often how they ask for it.

Common signs

- They live far away or overseas: on an oil rig, in the military, working as a doctor abroad.
- They always have a reason they can't video chat or meet in person.
- They move the conversation off the dating site to a private messaging app.
- An emergency comes up: medical bills, a customs fee, a plane ticket, a frozen account.
- They ask you to pay with crypto, gift cards or a wire, or to "invest" alongside them.

SCAM ALERT

The firm rule

Never send money, of any kind, to someone you haven't met in person. Not for a ticket, not for an emergency, not for an investment. A person who truly cares about you will understand.

Gentle ways to check

1. Search the person's name together with the word "scam."
2. Do a reverse image search of their photos. Pictures stolen from someone else's profile often turn up.
3. Tell a friend or family member about the relationship, and listen if they're worried.

TIP

There's no shame here

Romance scammers are skilled, and loneliness is human. If you think you've been caught in one, you can call the free AARP Fraud Watch Network Helpline at **877-908-3360** to talk it through with a trained specialist. See Chapter 29, *The Emotional Side, and Talking With Family* too.

CHAPTER 20

"Pig Butchering": Fake Crypto Investment Apps

"Pig butchering" is an ugly nickname, borrowed from the scammers themselves, for long-running crypto investment scams. The FBI calls it **cryptocurrency investment fraud**, and it was the largest source of reported losses to Americans in 2025. It often mixes friendship or romance with a fake investment.

How it usually goes

1. A "wrong number" text, a social media message, or a friendly person on a dating app starts chatting.
2. Over weeks, they mention how well they're doing investing in crypto, and offer to show you how.
3. They send a link to a trading website or app. It looks professional and shows your balance growing.
4. You may even be allowed to take out a small amount at first, to prove it's real.
5. When you try to withdraw more, you're told to pay "taxes," "fees" or a "deposit" first. The money never comes back.

The warning signs the FBI lists

- Someone you met online or through an unsolicited text pitches an investment.
- They ask to move the conversation to an encrypted messaging app.
- They promise high returns and pressure you to invest quickly.
- You're having trouble withdrawing your money, or you're told to pay new fees or taxes to get it out.

SCAM ALERT

Don't pay to withdraw

The FBI advises against paying any "fees" or "taxes" to release money from an investment platform. Paying more only adds to the loss.

The FBI may call you first

Through a program called **Operation Level Up**, the FBI finds people caught in crypto investment scams and contacts them directly, often before they realize anything is wrong. If someone says they're with the FBI, check that any email comes from an **@fbi.gov** address, and remember: the FBI will never ask you for money, ask you to move money to a new account, or ask for personal identifying information.

CHAPTER 21

Family Emergency, Utility, Prize and Job Scams

A few more stories also end at a Bitcoin machine. Each sounds different, and each breaks the same rule.

The story	What's really happening
Family emergency ("grandparent") scam	A panicked call from a "grandchild" or a "lawyer" who needs bail money right now. AI can even copy a loved one's voice. Hang up and call your family member on a number you know.
Utility shut-off	"Your power will be cut off in an hour unless you pay." The FTC says utilities never demand crypto. Call the number on your bill.
Prize or lottery	You've won, but must pay fees or taxes first. Real prizes don't charge you to collect them.
Job scams	An easy online job that pays well, but you must deposit crypto to "unlock" tasks or earnings. The FBI warns about these too.
Blackmail or sextortion	An email claims to have embarrassing videos and demands Bitcoin. Don't pay, don't reply, and change your passwords if they quote an old one.

SCAM ALERT

The common thread

Every one of these wants you to pay quickly, in a way that can't be undone. Slow down and verify. Nobody real will be harmed by you taking ten minutes to call someone you trust.

Couriers at the door

Some crews skip the machine and send a "courier" or "agent" to your door to collect cash or gold. The FBI has warned about this. If anyone says someone is coming to pick up money, don't open the door, and call 911.

TIP

A family code word

Some families agree on a private code word to use in a real emergency. If a caller claiming to be your grandson can't say it, you know. My guide *AI Voice Clones and Deepfakes* explains this in more detail.

CHAPTER 22

Red Flags at a Glance

Here's the whole part boiled down. If you notice even one of these, stop and talk to someone you trust before you do anything else.

Red flag	Why it matters
You're told to use a Bitcoin ATM or crypto kiosk	Only scammers demand this.
You're told to withdraw cash, especially a lot of it	Real problems don't get fixed with a pile of cash.
You're told to keep it secret, even from the bank	Secrecy protects the scammer, not you.
Someone sent you a QR code to scan	The QR code is the scammer's wallet.
You're asked to stay on the phone	They don't want you to think or call anyone.
A deadline: today, this hour, before the bank closes	Rushing is how scams beat common sense.
A new online friend talks about crypto profits	This is how investment scams start.
You're asked to pay "fees" to withdraw your money	A sign of a fake investment platform.
Someone offers to recover lost crypto for a fee	A second scam. See Chapter 28, *Recovery Scams: The Second Hit*.

STAY SAFE

When in doubt

Hang up, and call a number you already know: your bank, your family, or me at (330) 200-8042. A real organization will still be there in ten minutes. A scammer won't.

My guide *Spotting and Avoiding Scams* covers these warning signs for every kind of scam, not only crypto, if you'd like to go further.

GOOD TO KNOW

Caller ID can lie

A call can show your bank's name, the police department, or even "FBI" on the screen and still be a scammer. Never trust a caller just because of what your phone displays.

PART 4

If You Already Paid

What to do, in order, if money already went into a crypto machine: keep the evidence, call the kiosk company and your bank, report it, get Ohio help, and dodge the recovery scam that often follows.

CHAPTER 23

If You Already Put Money in a Bitcoin Machine

First, take a slow breath. You're not the first, you won't be the last, and it doesn't mean you're foolish. These crews are professionals. What matters now is doing a few things, in order, today.

Do these today, in this order

1. **Stop all contact.** Don't answer their calls or texts, and don't send any more money, no matter what they promise or threaten.
2. **Find the receipt** from the machine and keep it safe. Take a photo of it with your phone. See Chapter 24, *Your Receipt and Notes Are Evidence*.
3. **Call the company that runs the kiosk**, using the phone number printed on the machine or the receipt. Tell them it was a scam. See Chapter 25, *Call the Kiosk Company and Your Bank*.
4. **Call your bank** on the number on your card, especially if you withdrew cash or the scammers had access to your computer or accounts.
5. **Report it** to the FBI at **ic3.gov** and to the FTC at **ReportFraud.ftc.gov**, and file a report with your local police. See Chapter 26, *Report It: FBI, FTC and Local Police*.
6. **Tell someone you trust.** A family member, a friend, or me. You don't have to carry this alone.

HEADS UP

An honest word about getting money back

The FTC says that once crypto reaches a scammer, there's generally no way to get it back. Sometimes fast action can help, and law enforcement does sometimes trace and seize scam funds. But please go into this with clear eyes. Reporting still matters a great deal, for you and for the next person.

If the scammers were on your computer

If you let anyone connect to your computer, turn it off or unplug it from the internet, then use a different device to change your email and bank passwords. My guide *I Think I've Been Scammed* has a full first-24-hours plan for this, including freezing your credit.

SCAM ALERT

Expect them to call back

Scammers often return with a new story: "There's one more fee," or "We're the agency that recovers scam money." That's the same crew or their partners. See Chapter 28, *Recovery Scams: The Second Hit*.

CHAPTER 24

Your Receipt and Notes Are Evidence

The FBI says the most important information you can give investigators is the transaction details. Most of those are on the little paper receipt from the machine. Treat it like gold.

What to look for on the receipt

On the receipt	Why it matters
Amount	How much cash you put in, and how much crypto it bought.
Date and time	Exactly when the purchase happened.
Wallet address	The long string of letters and numbers where the crypto went. This is the scammer's address.
Transaction ID	Sometimes called TXID or hash. The payment's "receipt number" on the blockchain.
Kiosk company and location	The company that runs the machine and the store or address where it is.

Gather everything else, too

- Every receipt, if you went more than once or to more than one machine.
- Bank withdrawal slips or statements showing the cash you took out.
- The phone numbers that called or texted you, and the dates and times.
- Screenshots of texts, emails, chat messages, QR codes, websites or apps the scammers used.
- Names they gave, badge numbers, case numbers, "reference" numbers.

TIP

Don't delete, block

You can block a scammer's number without deleting their messages. Keep the messages for your reports. If a message makes you anxious, ask a family member to save screenshots for you.

Write a simple timeline

On a sheet of paper or in a note on your phone, write down what happened in order: the first contact, each call, each trip to the bank or machine. It doesn't have to be neat. It will make every phone call and report much easier, and you won't have to relive it from memory each

time.

GOOD TO KNOW

No receipt?

Report anyway. The FBI asks you to report even if you don't have every detail. Give the date, the store and the amount as best you remember, and ask the kiosk company what records it has.

CHAPTER 25

Call the Kiosk Company and Your Bank

Two calls belong near the top of your list: the company that runs the crypto machine, and your own bank. Make them as soon as you can.

Calling the kiosk company

The FTC's general advice for anyone who paid a scammer with cryptocurrency is to contact the company used to send the money, tell them it was a fraudulent transaction, and ask whether it can be reversed. For a crypto ATM, that's the company whose name is on the machine and the receipt.

1. Find the company's phone number or support website on the receipt or on the front of the machine. Don't search for it in an ad. Scammers buy ads that look like support lines.
2. Say, "I was the victim of a scam. I was told to use your machine." Give the date, time, amount and location.
3. Ask them to flag the wallet address as fraud, and ask whether anything can still be stopped or refunded.
4. Ask how to send them a copy of your police report, and write down the name of the person you spoke to and any case number.

HEADS UP

Keep your hopes modest, and be persistent

Most crypto ATM purchases are sent within minutes and can't be pulled back. The company may still be able to help in some cases. Ask clearly whether they have a fraud or refund process, keep notes, and follow up in writing.

Calling your bank

- Use the number on the back of your card or on your statement.
- Tell them you withdrew cash because of a scam, and whether the scammers had access to your computer, online banking or card numbers.
- Ask them to watch your account for unusual activity and to put extra protections in place.
- If scammers got your passwords, change them from a safe device.

GOOD TO KNOW

Why the bank still matters

Even if the crypto can't be reversed, the bank can help protect the money you still have, and some scams keep going for weeks. A heads-up may stop the next withdrawal.

CHAPTER 26

Report It: FBI, FTC and Local Police

Reporting can feel pointless when the money's gone. It isn't. Reports help investigators trace wallets, connect cases, warn others, and sometimes recover and return money. Here's where to go.

The three reports

Where	What to know
FBI Internet Crime Complaint Center	**ic3.gov**. The FBI asks crypto kiosk victims to include the transaction ID, the wallet address and the kiosk location, if available.
Federal Trade Commission	**ReportFraud.ftc.gov**. The FTC uses reports to track scams and build cases.
Local police	Call your police department's non-emergency number and ask to file a report. Bring your receipts, notes and timeline.

Filing at ic3.gov, step by step

1. Use a computer if you can. The form is long. Type **ic3.gov** yourself into the browser.
2. Choose to file a complaint, and answer the questions about yourself and what happened.
3. In the money section, enter each payment: the amount, the date, the wallet address and the transaction ID from your receipt.
4. Describe what happened in your own words, using your timeline.
5. Before you submit, print or save a copy of the finished complaint. Keep it with your other papers.

SCAM ALERT

The FBI never charges you

The IC3 will never ask for payment to recover lost funds, and it will never refer you to a company that charges to recover money. Anyone who says they're from the IC3 and asks for money is a scammer.

TIP

Need help filing?

If you're 60 or older, the U.S. Department of Justice's National Elder Fraud Hotline can help you report. See Chapter 27, *Ohio Help and Ohio's Crypto Kiosk Rules* for the number and hours.

CHAPTER 27

Ohio Help and Ohio's Crypto Kiosk Rules

Here in Ohio, you have help close to home as well as from Washington. Here's who to call, and where Ohio's rules on crypto machines stand as of November 2026.

Who to call

Who	How to reach them
Ohio Attorney General's Help Center	**800-282-0515**, Monday to Friday, 8 a.m. to 6 p.m. You can also file a complaint online at **OhioAttorneyGeneral.gov** or **OhioProtects.org**.
National Elder Fraud Hotline (U.S. Department of Justice)	**1-833-FRAUD-11** (1-833-372-8311), Monday to Friday, 10 a.m. to 6 p.m. Eastern, for people 60 and older.
AARP Fraud Watch Network Helpline	**877-908-3360**, Monday to Friday, 8 a.m. to 8 p.m. Eastern. Free, and open to AARP members and non-members.

Does Ohio limit crypto machines?

Some states have passed laws limiting how much money a crypto kiosk can take from a customer. In Ohio, a bill called the **ELDER Act (House Bill 648)** was introduced in the Ohio House in early 2026. As proposed, it would license crypto kiosk operators as money transmitters overseen by the state, set daily limits of $2,500 for new customers and $10,500 for existing customers, and add a 72-hour hold on transactions for new customers.

As of November 2026, I could not confirm that it has become law. The bill had sponsor testimony in the House Financial Institutions Committee in March 2026. Bills often change before they pass, so please don't count on any limit protecting you. The one rule in Chapter 2, *The One Rule That Stops Every Crypto ATM Scam* protects you no matter what any law says.

GOOD TO KNOW

Ohio AG complaints are public records

The Attorney General's office may share your complaint with the business involved, as part of trying to resolve it. That's normal. Include your receipts and timeline.

CHAPTER 28

Recovery Scams: The Second Hit

This is the cruelest part of crypto scams. After you've lost money, someone reaches out offering to get it back, for a fee. They might call themselves a crypto tracing company, a law firm, a government agency, or even the FBI. Paying them just means losing more.

What recovery scammers say

- "We traced your Bitcoin and found it. Pay a small fee to release it."
- "We're a law firm working with the FBI (or the FTC, or the IC3) to return scam victims' money."
- "Your case was assigned to us. Pay the processing tax in crypto or gift cards."
- Ads on social media promising to recover lost crypto, with glowing reviews.

SCAM ALERT

What the FBI says

The FBI has warned about fake law firms and "recovery" companies that target crypto scam victims. Red flags include claims of working with government agencies, requests for payment in crypto or gift cards, and fake letterhead. The FBI says there are no law firms that are officially authorized partners of U.S. government agencies.

Simple rules to stay safe

1. Government agencies never charge you to recover money, and never ask for crypto or gift cards.
2. Don't trust anyone who contacts *you* offering recovery. Real investigators contact you through your official report, and they don't ask for fees.
3. Never give remote access to your computer or share your banking details with a "recovery" service.
4. If you're unsure, call the agency yourself on a number from its official website, or call me.

HEADS UP

Scammers impersonate the IC3, too

The FBI has warned that scammers pose as IC3 staff to offer help getting money back. The IC3 doesn't make those calls asking for payment. If you filed a report and someone calls about it asking for money, hang up.

CHAPTER 29

The Emotional Side, and Talking With Family

Losing money to a scam hurts in two ways: the money, and the feeling that you should have known better. Please be as kind to yourself as you would be to a friend in the same spot.

Things worth remembering

- These scams are run by organized crews with scripts, training and fake documents. They fool doctors, lawyers, engineers and bankers.
- Feeling embarrassed is normal. It's also exactly what scammers count on to keep people quiet.
- Telling someone is how you protect the money you still have, and how you get support.
- Reporting helps catch the people who did this, and may protect a neighbor.

Telling your family

It can help to start simply: "I need to tell you something, and I need you to listen before you say anything. I was scammed." Most families respond with relief that you're safe and that you told them.

TIP

For family members

If a parent tells you they were scammed, your first words matter most. Thank them for telling you. Skip "How could you?" Focus on the next step together. Shame drives people back into silence, and silence is when scammers return.

People you can talk to

Who	How they help
AARP Fraud Watch Network Helpline	877-908-3360. Trained specialists offer guidance and support. They don't investigate or recover money, but they listen.
National Elder Fraud Hotline	1-833-372-8311, for people 60 and older.
988 Suicide & Crisis Lifeline	Call or text 988 if the loss feels like too much to bear. You matter more than any amount of money.

FROM BILL

You're welcome to call me

If you'd like help gathering receipts, filing your reports, or checking your computer and accounts, call or text (330) 200-8042. We'll go at your pace.

PART 5

Protecting Yourself & Your Family

A simple pause plan for your household, how to help a parent without taking over, answers to common questions, and how to reach me.

CHAPTER 30

Your Scam Pause Plan

The best protection isn't a gadget. It's a plan you make on a calm day, so you already know what to do when a scary call comes. It takes about ten minutes.

Make your plan

1. **Pick your "pause person."** One or two people you'll always call before moving any money: a son, a daughter, a friend, your banker.
2. **Write their numbers down** on paper by the phone, and save them in your phone's contacts.
3. **Write the one rule** on the same paper: *Nobody real sends me to a Bitcoin machine.*
4. **Write your bank's real number**, copied from the back of your card.
5. **Agree on a family code word** for real emergencies, so a fake "grandchild" can't fool you.
6. **Promise yourself one thing:** any request for money that comes with a deadline or a secret gets a call to your pause person first.

WHAT THIS DOES FOR YOU

Why it works

Scams depend on keeping you alone and hurried. A pause person breaks both at once. You don't have to decide whether it's a scam; you just have to make one call.

Practice the hang-up

Many of us were raised never to hang up on anyone. It may help to practice a sentence out loud, so it's ready when you need it: *"I don't handle money over the phone. I'll call back on a number I know."* Then hang up. You don't need to argue or explain.

TIP

Cut down on the calls in the first place

Fewer scam calls mean fewer chances to be fooled. My guide *Spam Calls and Robocalls* shows how to silence unknown callers and turn on your phone's scam protection.

GOOD TO KNOW

Ask your bank about extra protections

Many banks can set up alerts for large withdrawals or let you name a trusted contact they can reach if something looks wrong. Ask your bank what it offers; the options vary from bank to bank.

CHAPTER 31

Helping a Parent or Loved One

If you're a grown child or caregiver, you may be worried about a parent. The goal is to protect them while respecting that they're an adult who runs their own life. That balance matters: people who feel talked down to are more likely to hide things.

Start the conversation

- Share it as news, not a lecture: "I read that scammers are sending people to Bitcoin machines at gas stations. Have you ever gotten a call like that?"
- Share the one rule, and ask them to share it with their friends too.
- Offer to be their pause person, and make it clear they'll never be scolded for calling.

Signs a scam may be under way

- Unusual cash withdrawals, or several trips to the bank in a short time.
- Bitcoin ATM receipts, printed QR codes, or wallet addresses among their papers.
- Long, secretive phone calls, or a new online friend they won't talk about.
- Talk of a "case," a "federal agent," a "safe account," or a great crypto investment.
- Sudden stress, fear, or reluctance to let you see their computer or phone.

TIP

If you think it's happening right now

Stay calm. Ask questions rather than accusing. Offer to call the bank together using the number on the card. Show them this guide's Chapter 2, *The One Rule That Stops Every Crypto ATM Scam*. If they're in the middle of it, the most useful thing you can do is be the second voice they hear.

STAY SAFE

With their permission

Setting up account alerts, reviewing statements, or holding power of attorney are big steps. Do them openly, with your parent's agreement, and with the bank or an attorney's guidance. My guide *Helping a Parent From Afar* covers ways to help when you don't live nearby.

If you'd like a neutral person to sit down with your parent and walk through the warning signs, that's exactly the kind of visit I do. See Chapter 33, *When to Call Bill*.

CHAPTER 32

Questions People Ask About Crypto ATMs

Here are short answers to the questions that come up most about these machines and scams.

Question	Short answer
Is it illegal to use a Bitcoin ATM?	No. They're legal businesses. Using one because someone told you to is what makes it a scam.
Can the police make the kiosk company give my money back?	Usually not right away. The crypto has already left the machine. Reporting still helps investigators trace and sometimes seize funds.
The caller knew my name and bank. Doesn't that prove it's real?	No. Scammers buy personal details from data breaches and can fake caller ID.
They said the money is still mine, just "held in a safe wallet."	Whoever made the QR code owns that wallet. It's not yours.
Can I get my money back by paying a recovery service?	No. That's a second scam. See Chapter 28, *Recovery Scams: The Second Hit*.
The store clerk tried to warn me. Should I have listened?	Yes. Clerks and kiosk companies sometimes spot these scams. Next time, let them help.
Will I get in trouble for using the machine?	Being a scam victim is not a crime. Report it so you're on record as the victim.
Is crypto itself a scam?	Not by itself. But it's risky, uninsured, and the payment method scammers prefer. See Chapter 12, *Crypto Is Not a Bank Account*.

SCAM ALERT

"The FBI called to say I'm a victim."

The FBI does sometimes contact victims of crypto investment scams. But the real FBI never asks for money, never asks you to move funds, and never asks for personal identifying information. Any caller who does is an impostor.

A question for yourself

If you ever find yourself wondering, "Is this one of those scams?", the fact that you're asking is your answer. Pause and call someone. Real situations survive a phone call; scams don't.

TIP

Still have a question?

Call or text me at (330) 200-8042. I'd rather you ask than wonder.

CHAPTER 33

When to Call Bill

This guide is meant to help you stay safe on your own terms. But some situations are easier with a calm, experienced person beside you, especially when money and fear are involved.

Good reasons to call

- Someone told you to go to a Bitcoin ATM, and you want a second opinion before you do anything.
- You already put money in a crypto machine and want help gathering receipts and filing your reports.
- Scammers connected to your computer and you want it checked and cleaned up.
- A new online friend is talking about crypto profits and you want a neutral look at the website or app.
- You'd like your phone and computer set up to block scam calls and scary pop-ups.
- You're worried about a parent and want someone to explain the warning signs to both of you.

WHAT THIS DOES FOR YOU

Digital Safety Check-Up

This guide pairs with my **Digital Safety Check-Up**: an unhurried session where we go through your phone, computer, email and accounts together, tighten the settings that stop scam calls and pop-ups, and make your own scam pause plan.

SCAM ALERT

A two-minute call beats regret

If anyone is pressuring you to withdraw cash, buy crypto, or keep a secret, hang up and call me first at **(330) 200-8042**. I'll never ask you to move money, and I'll never ask for your passwords or codes over the phone.

How to reach me

I'm Bill, and Bill's Home Tech serves **Portage County, Ohio**. Call or text **(330) 200-8042**, or book online at **billshometech.com/book**. If you reach my assistant **Sophie** on the main line, she can answer simple questions and get you on my schedule. My help is **$49 remote · $99 in your home**. With 30+ years of professional experience, I promise there's no question too

basic.

STAY SAFE

In an emergency, call 911

If someone is at your door demanding money, or you feel threatened, call 911 right away. I'm here for questions, cleanup and peace of mind.

— Bill

CHAPTER 34

Your Crypto Scam Cheat-Sheet

The whole guide, boiled down to what you'll reach for most.

If someone is pushing you right now

If…	Do this
They say go to a Bitcoin ATM	Hang up. It's a scam, every time.
They say withdraw cash	Don't. Call your bank on the number on your card.
They say keep it secret	Tell someone right away.
They sent you a QR code	Don't scan it. That's their wallet.
A pop-up says call this number	Don't call. Close the browser or turn the computer off.
Someone is coming for cash	Don't open the door. Call 911.

If you already paid

Step	How
1. Stop contact	No more calls, texts or payments.
2. Keep the receipt	Photograph it. It has the wallet address and transaction ID.
3. Call the kiosk company	Number on the machine or receipt. Report fraud, ask about reversal.
4. Call your bank	Number on the back of your card.
5. Report	**ic3.gov**, **ReportFraud.ftc.gov**, and local police.
6. Get support	Ohio AG 800-282-0515 · Elder Fraud Hotline 1-833-372-8311 · AARP 877-908-3360

The short list

1. Nobody real sends you to a Bitcoin machine.
2. No bank, agency or company asks you to "protect" money by moving it.
3. Never share a recovery phrase, private key or one-time code.
4. Never send money to someone you haven't met in person.
5. Never pay a fee to withdraw an investment or recover lost money.
6. When in doubt, hang up and call your pause person.

Keep this handy

Keep handy	Fill in
My pause person	_____
Their phone number	_____
My bank's real number (from my card)	_____
Our family code word (keep it private)	_____
My local police non-emergency number	_____
Bill's Home Tech	(330) 200-8042 · billshometech.com/book

FROM BILL

You're ahead of the scammers now

You know what a crypto ATM is, how the scripts work, and exactly what to do if someone tries one on you. Share the one rule with a friend this week; it might save them a fortune. — Bill, (330) 200-8042